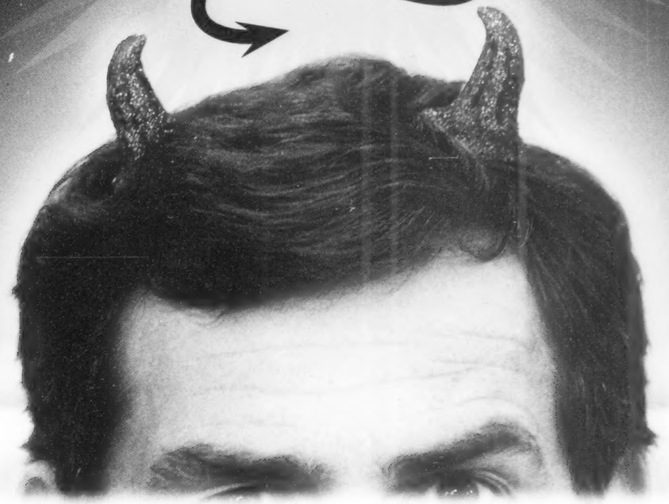
Also Inside: Facebook Reveals Data Center Secrets

Get Ready for the Tablet Invasion | Five Legal Risks in the Cloud

COMPUTERWORLD®

Peer Perspective. IT Leadership. Business Results. | COMPUTERWORLD.COM | APRIL 18, 2011

WHEN TRUSTED **IT PROS** GO **BAD**



One rogue sysadmin can do more damage than an army of hackers.

#BXBBJFT ***************CAR-RT LOT**B-050
#1292933/CB/0# 0000 003 21 040
1493-9
NA PUBLISHING, INC 69
PO BOX 998
ANN ARBOR MI 48106-0998

1,000 Oracle/Sun clients recently upgraded.

To IBM Power Systems.

Since 2009, over 1,000 clients have moved business to IBM Power Systems™ from Oracle/Sun. Some were swayed by the up to 60% drop in IT costs. Others by the 3x per core performance (per both TPC-C and SAP SD benchmarks). And some by both. Though all saw the strong business case for moving. We'd welcome the opportunity to show how IBM could help your organization, too.

ibm.com/facts

IBM®

IT COSTS: All client examples cited or described are presented as illustrations of the manner in which some clients have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual client configurations and conditions. PERFORMANCE: www.tpc.org as of 3/28/11 [IBM Power 780 (3 x 64 C)(24 Ch/192 C/768 Th); 10,366,254 tpmC; $1.38/tpmC; avail 10/13/10 v. Oracle SPARC SuperCluster w/T3-4 Servers (27 x 64 C)(108 Ch/1728 C/13824 Th); 30,249,688 tpmC; $1.01/tpmC; avail 6/1/11]. TPC-C is a trademark of Transaction Performance Processing Council. www.sap.com/solutions/benchmark/ as of 3/28/11 [IBM Power 795 (32 P/256 C/1024 Th); 126063 users/2-tier SAP ERP 6.0 pack4/AIX 7.1 + DB2 9.7; cert 2010046 v. Oracle SPARC Enterprise Server M9000 (64 P/256 C/512 Th); 39100 users/2-tier SAP ERP 6.0/Solaris 10, Oracle 10g; cert 2008042]. SAP is a registered trademark of SAP AG in Germany and several other countries. IBM, the IBM logo, ibm.com, DB2, Power Systems, Smarter Planet and the planet icon are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at www.ibm.com/legal/copytrade.shtml. © International Business Machines Corporation 2011.

COMPUTERWORLD

P.O. Box 9171
492 Old Connecticut Path
Framingham, MA 01701
(508) 879-0700
Computerworld.com

» **EDITORIAL**

Editor in Chief
Scot Finnie

Executive Editors
Mitch Betts, Julia King (events)

Managing Editors
Michele Lee DeFilippo (production),
Sharon Machlis (online),
Ken Mingis (news)

Director of Blogs
Joyce Carpenter

Art Director
April Montgomery

Technologies Editor
Johanna Ambrosio

Features Editors
Valerie Potter, Ellen Fanning (special reports), Barbara Krasnoff (reviews)

News Editors
Mike Bucken, Marian Prokop

Senior Editor
Mike Barton

National Correspondents
Julia King, Robert L. Mitchell

Reporters
Sharon Gaudin, Matt Hamblen, Gregg Keizer, Lucas Mearian, Patrick Thibodeau, Jaikumar Vijayan

Assistant Managing Editor
Bob Rawson (production)

Editorial Project Manager
Mari Keefe

Senior Associate Online Editor
Ken Gagné

Office Manager
Linda Gorgone

Contributing Editors
Jamie Eckle, Preston Gralla, Tracy Mayor

» **CONTACTS**

Phone numbers, email addresses and reporters' beats are available online at *Computerworld.com* (see Contacts link at the bottom of the home page).

Letters to the Editor
Send to letters@computerworld.com. Include an address and phone number for immediate verification. Letters will be edited for brevity and clarity.

News tips
newstips@computerworld.com

Subscriptions and back issues
(888) 559-7327, cw@omeda.com

Reprints/permissions
The YGS Group, (800) 501-9571, ext. 180, computerworld@theygsgroup.com

THIS ISSUE | 04.18.2011 [VOL. 45, NO. 8 $5/COPY]

24
LEGAL RISKS IN THE CLOUD

COVER STORY

When Trusted IT Pros Go Bad

18 One rogue IT staffer can do more damage than an army of hackers. These three horror stories could help you pick up on signs that a seemingly responsible employee is up to no good.

Legal Risks In the Cloud

24 Don't sign a contract until you consider five red flags in cloud service deals.

Forging a Virtual Steel Wall

30 Hardening software to prevent security breaches is coming back into fashion. And, yes, it's worth the trouble.

HEADS UP | **2** **Cyberwarfare** may affect unexpected targets. | The air transport industry gets a **"community cloud."** | **4** A fast-food chain builds a **know-how network.** | Status updates might be the new **spam.**

NEWS ANALYSIS | **6** Top vendors make new moves toward the **cloud.** | **8** Facebook shares specs for its new ultraefficient **data center.**

OPINIONS | **15** **Steven J. Vaughan-Nichols** thinks holding back Honeycomb is Google's biggest blunder yet. | **36** **Paul Glen** examines the three distinct experiences users have with IT. | **42** **Scot Finnie** warns that an irreversible tide of tablets is about to swamp the enterprise.

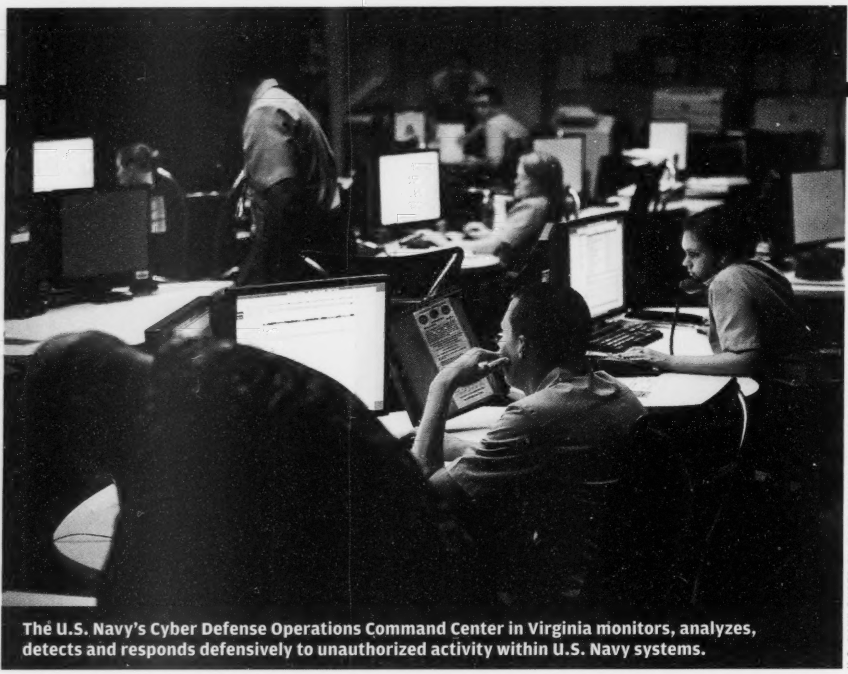
DEPARTMENTS | **10** **The Grill:** GlaxoSmithKline's Ingo Elfering. | **34** **Security Manager's Journal:** Keeping in-house code safe. | **38** **Career Watch** | **41** **Shark Tank**

FOR BREAKING NEWS, VISIT COMPUTERWORLD.COM

PHOTO ILLUSTRATION BY GETTY IMAGES

Fresh
Insights
New
Trends
Great
Ideas

HeadsUp



The U.S. Navy's Cyber Defense Operations Command Center in Virginia monitors, analyzes, detects and responds defensively to unauthorized activity within U.S. Navy systems.

U.S. NAVY PHOTO BY MASS COMMUNICATION SPECIALIST 2ND CLASS JOSHUA J. WAHL

SECURITY MONITOR

What Cyberwar Might Really Look Like

IMAGINE IT'S August 2020. A powerful and rising China wants to bring the city-state of Singapore into its fold like it has with Hong Kong. Before the first physical attacks, China launches a cyberoffensive to disrupt the communications capabilities of the U.S., Japan and their allies.

Members of the Chinese military's 60,000-strong cyberwarfare group deeply penetrate U.S. military, government and corporate networks. Crushing denial-of-service attacks hamper the Pentagon's efforts to mobilize conventional forces. Deliberately injected misinformation is sent to field commanders and to ships at sea.

That's a hypothetical scenario of how a full-scale cyberwar launched against the U.S by China might play out, and it's very different from conventional wisdom.

The scenario is described in a report by Christopher Bronk, a former U.S. diplomat and an IT policy specialist at Rice University's Baker Institute. The report was published in the latest issue of the U.S. Air Force's *Strategic Studies Quarterly*.

In an interview, Bronk downplayed popular visions of an "electronic Pearl Harbor," in which critical infrastructure, such as the electrical grid, is knocked out.

Such attacks can't be ruled out entirely, but it's unlikely that a nation-state would launch one, because of the catastrophic response it would trigger, he said.

Instead, Bronk said, cyberwar will be an effort "to get inside the other guy's decision process rather than shutting it off entirely."

– Jaikumar Vijayan

GET BREAKING NEWS AT
COMPUTERWORLD.COM

CLOUD SERVICES

Air Transport Industry Plans Private Cloud

SITA, the IT arm of the air transportation industry, is building a "community cloud" designed specifically for the industry's unique needs. The private cloud is scheduled to go live in June, the membership organization announced earlier this month.

The Air Transport Industry Cloud will be built on SITA's global network, which connects 90% of the world's airlines and 320 airports.

Depending on demand, the cloud will use six regional data centers on five continents, plus virtual data centers at large airports. SITA wants to ensure that end users experience response times of no more than 100 milliseconds.

The IT group plans to deliver desktop virtualization in June, followed by infrastructure as a service. SITA also plans to offer software as a service; available applications will include its baggage management system.

The cloud could help SITA and the air transportation industry cut costs by, for example, consolidating servers in regional data centers.

SITA estimated that the industry could save $40 million to $50 million per month if all eligible companies move their server infrastructures to the cloud.

Cloud services could also allow airlines to quickly adapt to industry changes – such as route expansions, disruptions or traffic spikes – at lower cost, SITA said.

– ANH NGUYEN,
COMPUTERWORLD U.K.

YOUR BUSINESS IS UNIQUE.
YOUR PATH TO CLOUD SHOULD BE, TOO.

Move beyond.

Moving beyond means building a competitive edge into your IT infrastructure. An edge that makes you more flexible, enables a more agile enterprise and, above all, is uniquely yours. Through our industry-leading virtualization and cloud infrastructure solutions, we can help you move beyond—to your cloud, where accelerated IT delivers accelerated results for your business.

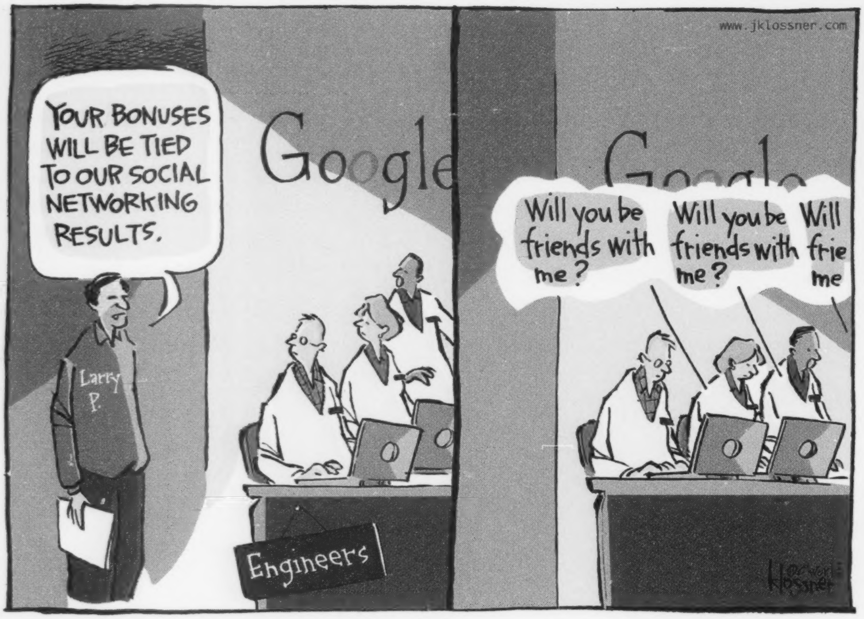
vmware.com/movebeyond

vmware

© 2011 VMware, Inc. All rights reserved.

BETWEEN THE LINES

By John Klossner


www.jklossner.com
YOUR BONUSES WILL BE TIED TO OUR SOCIAL NETWORKING RESULTS.
Google
Larry P.
Engineers
Google
Will you be friends with me?
Will you be friends with me?
Will frie me
Klossner

IT STRATEGY

IT Leader Builds a Know-how Network

DICKIE OLIVER is on a mission to build an enterprise "know-how platform" so that 1.6 million employees across 110 countries can do a better job of selling chicken, pizza and tacos.

Oliver is vice president of global IT at Yum Brands, the $11 billion owner of the KFC, Pizza Hut and Taco Bell restaurant chains.

In a highly competitive business, Yum has to continually generate profitable new ideas for domestic and international markets. Oliver said in an interview that he has a four-point IT strategy for getting employees at his "very spread-out global company" to break out of silos and share know-how. It includes the following elements:

- An internal social network, called iChing, based on the Jive software platform. Employees use the network to post documents, ask questions, collaborate and learn about successful strategies in other areas.
- Enterprise search technology from Coveo layered on top of iChing and other data repositories. This provides a user-friendly tool that employees use to glean insights from unstructured and structured data. In essence, the search technology stitches together multiple information sources without expensive data integration.
- A Saba online learning system that lets employees across the planet participate in training and webinars in several languages, eliminating the need for trips to the U.S.
- A high-definition Tandberg videoconferencing system that lets employees have virtual meetings so they don't have to travel as much.

Krushers, a slushy drink that tested well in Australia, is an example of an innovation that the new platform helped nurture, said Oliver. The concept was posted on the iChing network, which led to other markets rolling it out quickly and with great success, he said.

The next step, now in beta, could be using the Coveo search capability to pull information from various systems to provide a consolidated, 360-degree view of each employee and present it to managers in a single dashboard.

– Mitch Betts

Micro Burst

DATA HAVENS

A survey finds that

70%

of organizations that store sensitive data abroad choose countries with weak privacy laws.

SOURCE: McAFEE/SAIC SURVEY OF 1,000 IT DECISION-MAKERS, MARCH 2011

HUMAN FACTORS

Danger Ahead: A Deluge of Status Updates

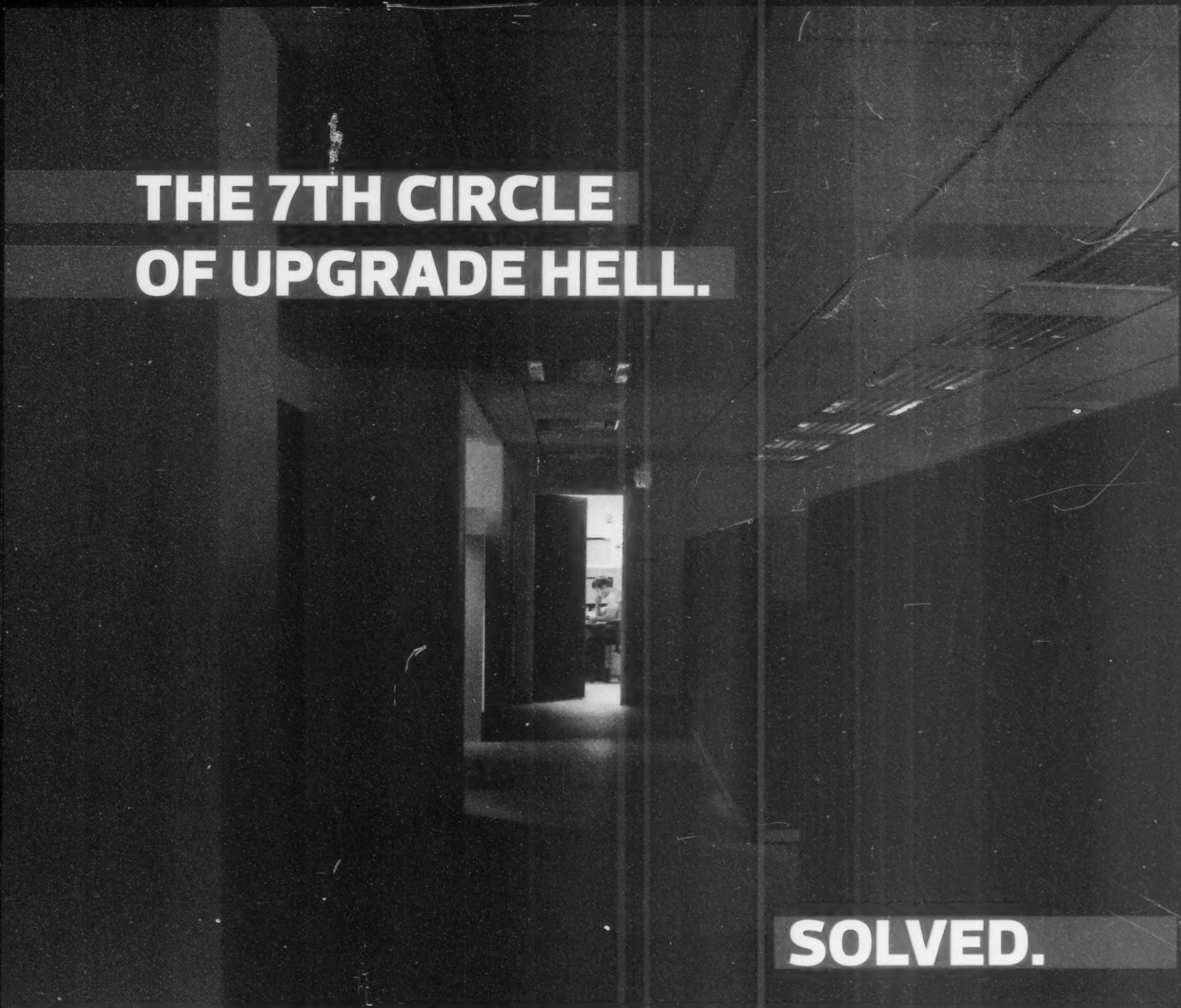
If you think email overload is bad, just wait until employees are hit with "activity streams" that combine status updates from various corporate systems and social networks into a single feed.

"Activity streams have been around a while as a concept but are getting a bump in interest," noted Gartner analyst Craig Roth in a blog post last month. "IBM talked them up at Lotusphere 2011. Microsoft added an ActivityManager in SharePoint 2010." One vendor, SocialCast, views an activity stream as a corporate "central nervous system" that enhances collaboration.

But Roth said he envisions an overwhelming series of updates from customer relationship management systems ("Jim just hit his sales quota"), content management systems ("Presentation AugConfv2.pptx was added"), social networks ("Jackie commented on Susan's photo"), and project planning systems ("Task 'Get buy-in from VPs' is now 2 days overdue").

"The resulting deluge of status updates may give activity streams a bad name," Roth said. He urged vendors to include alerts, filters and recommendation engines so end users can determine what merits their attention.

– MITCH BETTS



We get the devil is in the details. We'll sort through the latest software versions, simplify licensing agreements, even tell you when you don't have to upgrade at all. And our partnership with Adobe brings you the unique software solutions you need to create and deliver compelling content. So your upgrades bring results, not nightmares.

Salvation awaits at CDW.com/adobe

Adobe + CDW PEOPLE WHO GET IT™

©2011 CDW LLC. CDW®, CDW·G® and PEOPLE WHO GET IT™ are trademarks of CDW LLC.

cloud
control
option
alt
return

Top Tech Vendors Renew Cloud Push

IBM, Dell and HP unveil tools aimed at convincing IT execs that cloud services can be secure and reliable.

By James Niccolai and Patrick Thibodeau

LOOKING TO ALLAY corporate IT misgivings about hosted computing services, IBM and Dell earlier this month unveiled tools that focus on helping companies build and use more secure and reliable private and public clouds.

The IBM and Dell announcements came just weeks after Hewlett-Packard announced a so-called infrastructure-as-a-service (IaaS) cloud offering for both consumers and businesses.

IBM introduced two tiers of cloud services under the name SmartCloud, while Dell announced plans to spend $1 billion this year to build data centers that support cloud services for corporate customers. Dell also said it's building preconfigured, pretested and pre-validated systems to help customers create in-house private clouds.

Dell is likely to focus initially on small to midsize users.

IBM's Enterprise IaaS offering lets customers deploy Windows- or Linux-based software from IBM data centers with 99.5% uptime guaranteed. Its Enterprise Plus service has additional security and promises 99.9% uptime.

The company is looking to further attract the attention of enterprises by adding support for high-end SAP ERP applications. Ric Telford, vice president of cloud services at IBM, said that the cloud offering will let SAP users dynamically provision instances on demand, and it will elastically scale. IBM has also bundled hardware and management software products, including numerous Tivoli and Systems Director tools, so they can be run from an internal cloud.

"There's nothing about the attributes [of cloud services] that you can't implement inside a business," said Steve Mills, senior vice president and group executive in charge of IBM's software division.

Given that even the IBM customers who attended the company's Cloud Forum event in San Francisco earlier this month are either not yet using cloud-based services or are still in the early stages, analysts say the strategy makes sense.

Tony Kerrison, CTO at financial services firm ING, said his company runs "zero" applications today that are hosted in the public cloud.

Like other financial services companies, Amsterdam-based ING is heavily bound by regulatory requirements, and by strict European Union rules about where its customer data can be stored. Even putting email in the cloud, which is first on Kerrison's wish list, will be "a challenge" because of the regulatory issues, he said in an interview at the IBM event.

Meanwhile, health care company Kaiser Permanente "dipped [its] toes" into cloud computing this year, said Carlos Matos, senior director for infrastructure management and systems integration. Scott Skellenger, senior director for global IT operations at life sciences firm Illumina, declined to say what, if any, applications his company is running in the cloud.

Other top vendors still have a window of opportunity to make a serious push into the cloud computing business. The cloud services market is "highly fragmented," said IDC analyst Matt Eastwood. "There is still room for everyone." ◆

Niccolai *is a reporter for the IDG News Service.* **Robert McMillan** *of the IDG News Service contributed to this story.*

> There's nothing about the attributes [of cloud services] that you can't implement inside a business. — STEVE MILLS, SENIOR VICE PRESIDENT AND GENERAL MANAGER, IBM

© FOTOLIA / JAKUB JIRSÁK

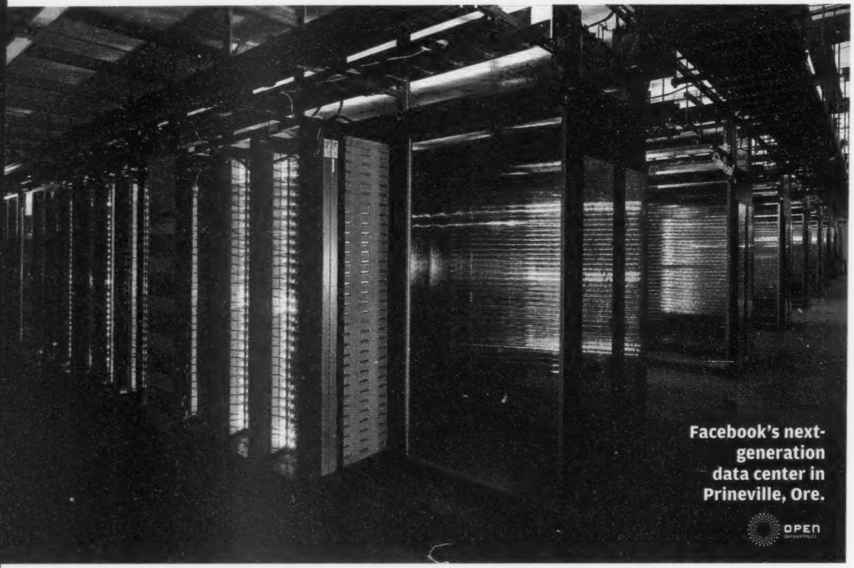
vmware
WE PUSHED INNOVATION.
ALL YOU HAVE TO DO
IS PUSH THE 'ON' BUTTON.
vStart

vStart virtualization from Dell.

It really is that simple. vStart from Dell takes the complexity and time out of virtualizing your enterprise by delivering it at the push of a button. Pre-configured servers, storage, networking and VMware software managed via a single console can be deployed in hours not days. And it's just as simple to find out more by going to www.dell.com/vstart or join the conversation at #vstart on Twitter.

Efficient Enterprises do more with Dell.
dell.com/vstart

DELL
The power to do more



Facebook's next-generation data center in Prineville, Ore.

Facebook Reveals Its Data Center Secrets

The social networking leader shows why its new Oregon data center is said to be one of the most efficient in the world. By Robert McMillan and Sharon Gaudin

FACEBOOK this month revealed some of the secrets behind its new next-generation data center, an IT facility in rural Prineville, Ore., that some experts say is one of the world's most efficient.

As part of the company's Open Compute Project, Facebook officials released specifications for the data center's custom-built rack-mounted servers, which they said weigh less and use more-efficient power systems than most others do. The company also disclosed its methods for cooling racks of servers without air conditioning.

The technical details are posted on the OpenCompute.org website hosted by Oregon State University's Open Source Lab.

The site explains the design of the server chassis and lists the specifications for the components used in the systems, including their AMD Opteron- and Intel Xeon-based motherboards and their power supplies.

Facebook and its Open Compute Project partners — Advanced Micro Devices, Intel and Quanta — have been tweaking and tuning the data center specifications for about a year while working with server makers like Dell, Hewlett-Packard, Rackspace, Skype and Zynga to build lighter, cooler systems that are easy to repair.

"These servers are 38% more efficient than the servers we were buying previously," said Jonathan Heiliger, vice president of technical operations at Facebook. The finished product also costs some 24% less than the industry average for similar servers, he added.

The bare-bones boxes aren't much to look at — Facebook calls the design "vanity-free" — but they get the job done. The company says the Prineville data center has a 1.07 Power Usage Effectiveness rating. Developed by the Green Grid consortium, PUE is a standard measurement for data center efficiency. The Prineville facility's 1.07 rating is well below the industry average of around 1.5, meaning it is far more efficient than most data centers.

Facebook's custom servers are about 6 pounds lighter than typical rack-mounted systems, but they're thicker. While most server racks are 1U (1.75 in.) thick, Facebook's are about 1.5U, so engineers can squeeze in taller heat sinks with more surface area and larger, more efficient fans. That means less air has to be pumped through the servers to cool them.

"We're not selling anything today, but we do hope to benefit from this — primarily in the area of accelerating innovation," said Frank Frankovsky, director of hardware design at Facebook.

Prineville's central Oregon location should help in Facebook's energy-saving efforts, City Manager Steve Forrester told *Computerworld* earlier this year. The city sits on a plateau at an elevation of 2,860 feet, where it's possible to use outside air to cool systems for more than half of the year, Heiliger said in a blog post.

Zeus Kerravala, an analyst at Yankee Group, said the fact that Facebook has enough clout to drive hardware innovation says a lot about how far the company — and the social networking sector in general — have come. "If anybody still doubted the validity of social networking," he noted, "this kind of takes care of that." ◆

McMillan *is a reporter for the IDG News Service.* Computerworld*'s* **Patrick Thibodeau** *contributed to this story.*

> **We're not selling anything today,** but we do hope to benefit from this – primarily in the area of accelerating innovation. – FRANK FRANKOVSKY, DIRECTOR OF HARDWARE DESIGN, FACEBOOK

workday.

LEGACY ERP
THE CLOUD

Your ERP system was built more than 20 years ago, when your PC had 4 megs of memory and a mobile phone was the size of a brick. You're trapped on an old version of software that is difficult to update, costing you millions in maintenance fees and even more for bolt-on technologies that make your systems barely usable.

The cloud changes everything. When you run your business applications in the cloud, you are embracing a technology revolution and the competitive advantage that comes with it. Only cloud computing can deliver innovation at a pace that matches today's global business—at half the cost of upgrading your current ERP system.

Human Resources, Payroll, and Financials in the cloud

www.workday.com

BUSINESS, **REINVENTED**

THE Grill

Ingo Elfering

A global view helps this IT leader read cultural differences in diverse teams.

What futuristic technology would you love to see become reality? More intuitive user interfaces.

What did you want to be when you were in high school? I was always fascinated by technology. Literally I wanted to become a rocket scientist. But I started my own company at 16.

What new place would you like to visit? Although I'm doing a project in Nigeria, I've never set foot in Africa; that's on my list to change in the not-too-distant future.

Best piece of advice you've ever gotten: There are two. Hug your problems, because they're opportunities for improvement. And you can change only yourself, but you control that 100%.

PHOTOGRAPHY COURTESY OF GSK

INGO ELFERING *talks a lot about opportunities. That's not surprising, considering he has built his career on developing transformative uses for IT. In 1987 he founded his own company, MedicalData Service, which developed software for the medical community. SmithKline Beecham bought Elfering's company in 1997 and hired him as part of the deal. A native of Germany, he came to the U.S. with his wife in 2000 when a merger created GlaxoSmithKline. Last November, Elfering became vice president of business transformation for the company's Core Business Services. He now holds dual American and German citizenship and was named one of* Computerworld's *2010 Premier 100 IT Leaders.*

You describe yourself as "an innovator and change agent." How do those characteristics show in your day-to-day job? We do these big projects around innovative things, or big programs that take years to accomplish or are global in scale, so you have to drive

Continued on page 14

Microsoft

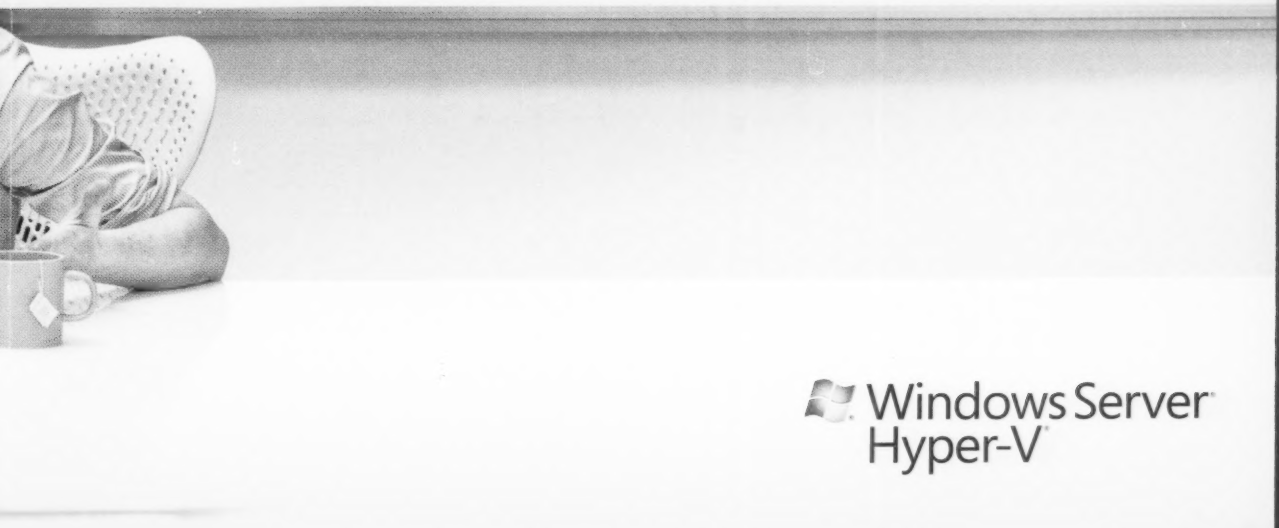
Still just talking virtualization?

Microsoft
Cloud Power

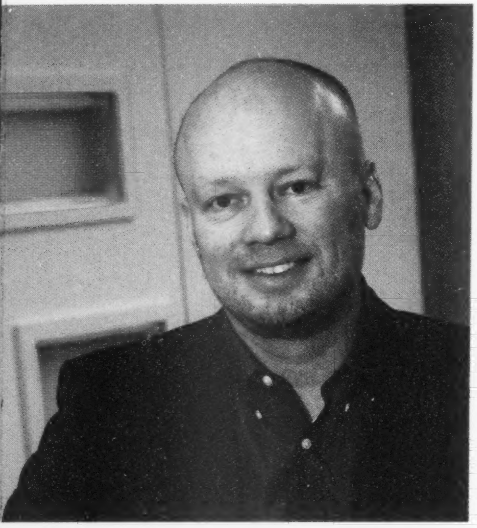
Now we're talking private cloud.
Windows Server is changing the conversation.

Windows Server Hyper-V and **System Center** let you manage your infrastructure as a private cloud: a pool of computing resources that lets you allocate computing power to your applications as your business requires. And Microsoft provides common management, identity and development tools that work across your infrastructure. End-to-end control. Agility beyond virtualization.
That's Cloud Power.

Find out more about our private cloud solutions.
Microsoft.com/cloud/privatecloud
Text COMP2 to 70700* or scan our tag.
Get the free mobile app from http://gettag.mobi
*Standard messaging and data rates apply.



Windows Server
Hyper-V



> “**If you can translate what the business opportunities are and how IT can support that,** that’s where people can make the real difference.

Continued from page 10

change, but more important to me is to be open every day and look externally. Bring innovation in everything you do, not just the big projects. Scan the market externally in your own field, but also in other businesses. Opportunities can come from the strangest places. I was reading about mobile phones and banking in Africa, and a little while later we started [a project using mobile phones] in Nigeria. People buy our products and they scratch off something on the side of the box, and they see a number that they can text to a service center for us, and we can track that number and show it’s unique and that the product is produced by us. It’s a great way for us to ensure patients that what they’re getting is genuine medication.

You’re in a very specific industry. Do you think CIOs need deep industry knowledge, particularly when working in specialized fields? It helps a little bit, but more important is the ability to embrace change. I think your ability to learn is more important than specific industry knowledge, and a part of that is because your knowledge, particularly in IT, can change very quickly. There is something about the speed of innovation that’s particularly important in IT. You have to continue your education and stay up to date and find new innovations and opportunities. When you do that, you really have something to contribute to the business. If you can translate what the business opportunities are and how IT can support that, that’s where people can make the real difference.

So many companies, even small ones, are global today. What are the top challenges for IT when working across different companies, countries and cultures, with all their different regulations and requirements? The regulations and requirements and the global scale, they do bring their own specific challenges, like how do you make something comply to different privacy regulations around the world and be in compliance with all of them?

But I think in the project environment, the more challenging aspect is the cultural differences. If you have a team spread out across four or five different locations, you can’t just walk down the hall anymore and talk to somebody or get everybody into a huddle in the morning. And even if everyone speaks English, they might not talk about the same thing. We had a meeting where there was a lot of confusion about what we meant by a word. We spent half an hour explaining what the word was and our meaning around it.

What was the word? Sourcing.

So how do you deal with cultural differences in a global team? I have a personal benefit. I’ve worked long enough in the U.S., and I’m German, and I’ve worked in nearly every European country, so I’m more attuned to the cultural differences. And what my experience taught me is you have to have that internal awareness, and ask lots of questions and be someone who teases out these differences and says, “This is what I think you’re talking about,” or, “There might be an understanding gap here.” That really becomes helpful for teams.

Sounds like this is helpful for all teams, not just ones from diverse locales. Absolutely. My *sourcing* example was with people from the U.S. and U.K. They all spoke English. But there were at least six different definitions of what *sourcing* means. I sometimes joke about this because when you only have a hammer, everything looks like a nail, and you have to understand when you’re looking at a nail or when you’re looking at a screw. You have to train yourself to constantly have that awareness. You have to always ask questions, and you can come down to a deep understanding of what’s really meant or why something is really happening.

You’ve talked about driving change during this recession. What about driving change in a good economy? In good times, you should have even more of a desire to drive and implement change because you are less forced and maybe have an opportunity to invest. You might have some upward pressure and growth you can build on. I’ve seen the need to innovate and change constantly. So it’s not a question of when; it’s how. The tools might vary slightly whether it’s an upturn or downturn, but technology changes and innovation keeps happening, and you should be driving that and driving it forward, and you do it all the time.

— *Interview by* Computerworld *contributing writer*
Mary K. Pratt *(marykpratt@verizon.net)*

OPINION

S.J. VAUGHAN-NICHOLS

Google's Blunder

I DON'T SAY THIS VERY OFTEN, but some days Google is stupid. Until recently, Google's biggest blunder was Google Wave. But now Google has announced that it won't release Android 3.0, the tablet version of its mobile operating system, until it has made it "better."

> Google says it won't release Android 3.0, Honeycomb, until it has made it 'better.' This has ticked off pretty much every open-source professional.

In a statement, Andy Rubin, head of Google's Android group, said, "Android 3.0, Honeycomb, was designed from the ground up for devices with larger screen sizes and improves on Android favorites. . . . While we're excited to offer these new features to Android tablets, we have more work to do before we can deliver them to other device types, including phones." In other words, Google will release the Honeycomb source code as soon as it's ready. Just don't ask when that will be.

This has ticked off pretty much every open-source professional out there. Android is under the open-source Apache Software License 2.0, which requires that the source code be released when the executable programs are released. That usually means they're released together. But the license doesn't insist on that.

Historically, Google has played games with the ASL's terms by letting big hardware manufacturers, such as HTC, Motorola and Sony, have an early look at Android source code. Smaller vendors, developers and open-source purists have been unhappy with that "some animals are more equal than others" approach in the past, and now Google is stretching the gap between private release and an open-source release even further. Some would say it has stretched the gap to the breaking point.

I know Google doesn't want vendors rushing half-baked Honeycomb tablets out to the public. But you know what? I'd rather see tiny companies trying to make a fast buck by selling not-ready-for-public-consumption tablets than a big company playing games with open-source licensing.

Google already has enough intellectual property troubles, with Oracle suing over Java, Microsoft creeping toward a suit, and an assortment of open-source-related copyright claims. Does it really need to alienate the programmers? I think not.

What really troubles me, though, isn't Google playing fast and loose with the ASL. No, what bugs me about this, and what makes it one of Google's all-time dumb moves, is that the whole point of open source is that you might make your life easier by sharing the code. Right now, all of Honeycomb's development rests on a relative handful of in-house Honeycomb developers. The big OEM developers will be spending their time adding gewgaws to the base code. They're not going to help get Honeycomb out the door.

By turning its back on open source, Google is not only harming and annoying other Android developers. It's also hurting its own operating system, and its own future.

I don't know who came up with this idea at Google, but I do know he was an idiot. In 2011, even Microsoft, enemy of all things open, has realized the worth of open source as a development method. Google itself rests on Linux. To decide that turning the developer clock back 20 years is the right move strikes me as foolish beyond belief.

Even so, since Apple has shown no interest in the low-end or midrange tablet markets, and since no one else is really ready to enter them, I'm sure Honeycomb will be a success. I'm also sure it will be filled with more bugs than it would have been if Google had kept the code open. If Google continues on this path, Android may eventually face real challenges from webOS, Windows Phone 8 or even Windows 8. I can only hope Google realizes the error of its ways — for its own sake, if not for the sake of its smaller developer partners and customers — in time to keep Android a top mobile operating system. ◆

Steven J. Vaughan-Nichols has been writing about technology and the business of technology since CP/M-80 was cutting-edge and 300bps was a fast Internet connection – and we liked it! He can be reached at sjvn@vna1.com.

CUSTOMER VIEWPOINT

Jeff Porter

DIRECTOR OF IT INFRASTRUCTURE, FAIRFAX COUNTY, VA.

Jeff Porter has spent more than 29 years in the IT industry working in different roles in both the public and private sectors. Currently he manages the Infrastructure Platform Division for Fairfax County Government. He is responsible for the overall management of the IT service desk, desktop support, server support, database support, Microsoft Exchange, Microsoft System Center Configuration Manager, antivirus support, storage and remote access.

FOR MORE INFORMATION: please visit us at citrix.com/simplicityispower

BLOG: http://twitter.com/citrixblogs

TWITTER: citrix.com/twitter

More Bang, Fewer Bucks

A government IT executive explains how technologies such as virtualization and cloud computing are stretching tight IT budgets.

Located due west of Washington D.C., Fairfax County, Va., is one of the largest counties in the United States, with more than 1 million residents, some 12,000 government employees—and a drum-tight IT budget. We asked Jeff Porter, the county's director of platform technologies, to share his thoughts on strategies for doing more without spending more.

Everyone faces budget pressures these days. How can virtualization help in addressing them?

Like many othere state and local governments, we've seen revenues decline in recent years and demand for services go up. So we've had to find innovative ways to get much more efficient. Virtualization has been one of our most successful strategies. Using virtualization, we've consolidated 600 physical servers down to just 12. That's helped us drastically cut hardware spending and maintenance overhead, because we don't have as many physical devices to manage. In fact, we expect to save roughly $3 million just on server procurement over the next two years, and about another $200,000 on energy. Also, virtualizing our desktops has enabled us to extend the life of our PCs. As a result, we've taken $2.5 million a year that used to fund new hardware purchases and reallocated it to funding innovative new services instead. That's more than just a win for IT. It's a win for the entire county.

> "We've taken $2.5 million a year that used to fund new hardware purchases and reallocated it to funding innovative new services instead. That's more than just a win for IT. It's a win for the entire county."

Spending is one side of the efficiency equation, but does virtualization contribute to productivity as well?

It certainly has in our case. Unlike private businesses, governments can't close up shop due to heavy snowfall, a flu epidemic or some other emergency. Those are actually the times when people need us most. Using desktop virtualization, we've made it much easier for county employees to work from home, so they can continue serving citizens even when they can't make it into the office for some reason. In fact, we've made it so easy to work from home that lots of people are doing that even when there's no emergency. We call them "day extenders," because they use a virtual desktop to sneak in a few extra hours of work after dinner or on the weekend.

What role can cloud computing play in stretching an IT budget?

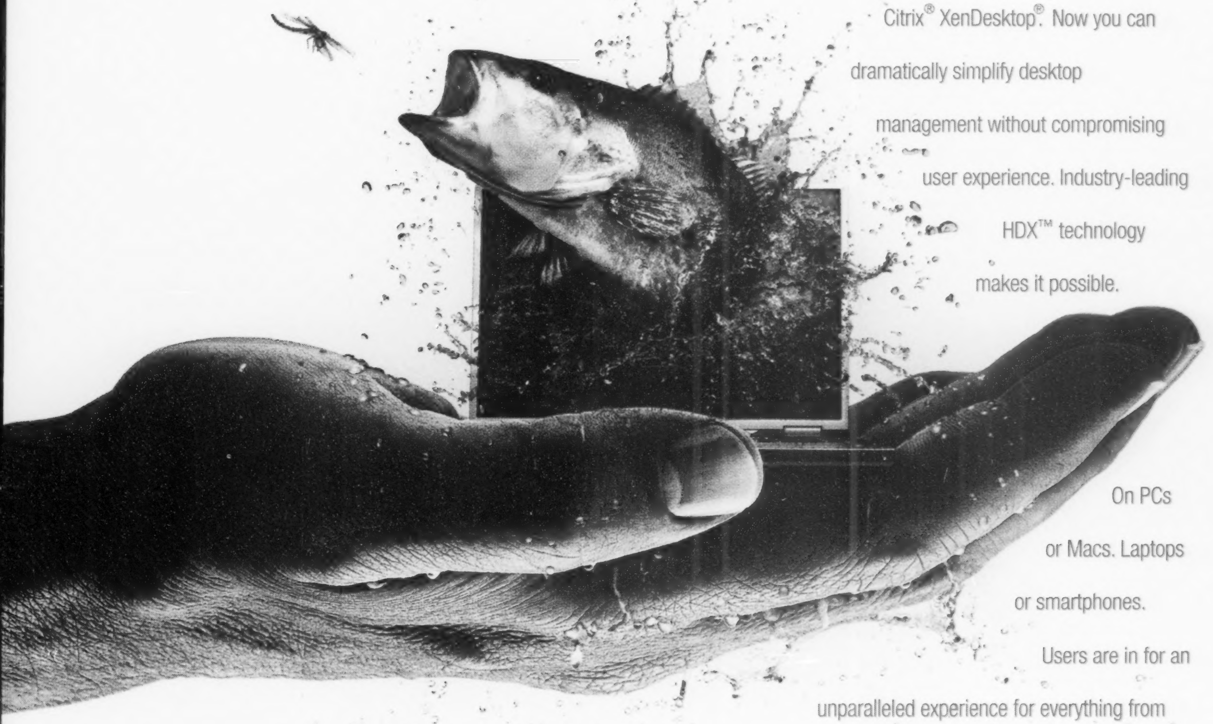
Fairfax County is 400 square miles in size, and sometimes sending a technician out to install or remove desktop software takes too long. So we're using an internal cloud infrastructure to power a software-as-a-service (SaaS) environment. County employees who need a new application can now file a request online. If their boss approves it, they can then complete the installation on their own. We're also doing this for operating systems. We run mostly Windows XP at present, but if someone wants to upgrade to Windows 7, they can do that on their own via the internal cloud.

How do you keep all of that secure?

Very few of our end users have administrator rights to their machine, so the only way they can add new software is through our online self-service environment. That enables us to monitor new installations and keep the entire process safely inside our firewall. So we get better efficiency and better security in one package. It's the best of both worlds.

COMPUTERWORLD
Custom Solutions Group

CITRIX®



SIMPLICITY IS POWER

The power of virtual computing in high-def.

It's more than a desktop. It's an immersive virtual computing experience. Deliver a vibrant, personalized, high-definition desktop to any device, across any network, with Citrix® XenDesktop®. Now you can dramatically simplify desktop management without compromising user experience. Industry-leading HDX™ technology makes it possible.

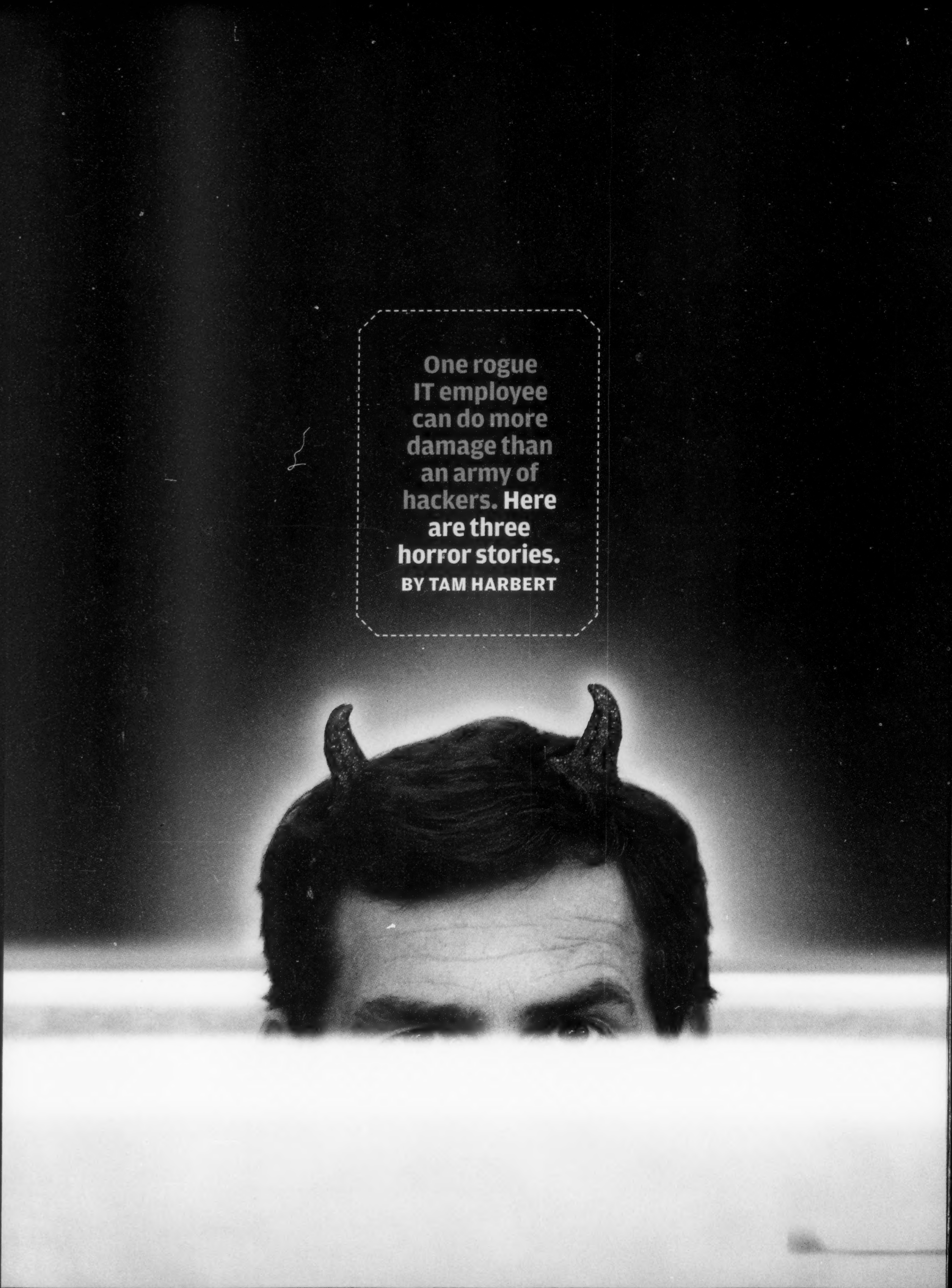
On PCs or Macs. Laptops or smartphones. Users are in for an unparalleled experience for everything from applications to rich media. That's the power of virtual computing at work. And everywhere else, too.

Simplicity is power. Citrix.

CITRIX®

Citrix.com/SimplicityIsPower

© 2011 Citrix Systems, Inc. All rights reserved. Simplicity is Power and its stylized treatment, XenDesktop and HDX technology are trademarks and/or registered trademarks of Citrix Systems, Inc.



One rogue IT employee can do more damage than an army of hackers. **Here are three horror stories.**

BY TAM HARBERT

WHEN TRUSTED **IT PROS** GO BAD

IT'S A CIO'S WORST NIGHTMARE: a call from the Business Software Alliance, saying that some of the software your company uses might be pirated.

You investigate and find that not only is your software illegal, it was sold to you by a company secretly owned and operated by none other than your own IT systems administrator, who's been a trusted employee for seven years. When you start digging into the admin's activities, you find a for-pay porn website he's been running on one of your corporate servers. Then you find that he's downloaded 400 customer credit card numbers from your e-commerce server.

And here's the worst part: He's the only one with the administrative passwords.

Think it can't happen? It did, according to a security consultant who was called in to help the victim, a $250 million retailer in Pennsylvania. You never heard about it because the company kept it quiet.

Despite the occasional headlines about IT folks gone rogue, most companies

NOEL HENDRICKSON / GETTY IMAGES

sweep such situations under the rug as quickly and as quietly as possible.

An annual survey conducted by *CSO* magazine, the U.S. Secret Service and CERT (a program of the Software Engineering Institute at Carnegie Mellon University) routinely finds that three quarters of companies that are victimized by insiders handle the incidents internally, says Dawn Cappelli, technical manager of CERT's Insider Threat Center. "So we know that [what's made public] is only the tip of the iceberg," she says.

By keeping things quiet, however, victimized companies deny others the opportunity to learn from their experiences. CERT has tried to fill that void. It has studied insider threats since 2001, collecting information on more than 400 cases. In its most recent report, which analyzes more than 250 cases, CERT says the most common mistakes include failing to vet job applicants thoroughly, neglecting to adequately monitor the process of granting access privileges, and overlooking red flags in behavior.

But the threats posed by privilege-laden IT employees are especially hard to recognize. For one thing, staffers' nefarious activities can look the same as their regular duties. IT employees routinely "edit and write scripts, edit code and write programs, so it doesn't look like anomalous activity," Cappelli says. They know where your security is weakest and how to cover their tracks.

Victimized companies typically won't talk, but security consultants who help clean up the messes sometimes do. We talked to three security pros who shared these stunning tales of rogue IT employees.

CERT's Dawn Cappelli says IT safeguards and routine vigilance offer the best protection against insider threats.

Pirating Software — and Worse

The Pennsylvania retailer's tale of woe began in early 2008, when the BSA notified it that Microsoft had uncovered licensing discrepancies, according to John Linkous. Today, Linkous is chief security and compliance officer at eIQ Networks, a security consultancy. His experience with the incident involving the retailer is from his previous job, when he was vice president of operations at Sabera, a now-defunct security consultancy.

Microsoft had traced the sale of the suspect software to a sysadmin at a company that was a Sabera client. For the purposes of this story, we'll call that sysadmin "Ed." When Linkous and other members of the Sabera team were secretly called in to investigate, they found that Ed had sold more than a half-million dollars in pirated Microsoft, Adobe and SAP software to his employer.

The investigators also noticed that network bandwidth use was abnormally high. "We thought there was some kind of network-based attack going on," says Linkous. They traced the activity to a server with more than 50,000 pornographic still images and more than 2,500 videos, according to Linkous.

In addition, a forensic search of Ed's workstation uncovered a spreadsheet with hundreds of credit card numbers from the company's e-commerce site. While there was no indication that the numbers had been used, the fact that the information was in a spreadsheet implied that Ed was contemplating using the card data himself or selling it to a third party, according to Linkous.

The retailer's chief financial officer, who had originally received the call from the BSA, and others on the senior management team feared what Ed might do when confronted. He was the only one who had certain administrative passwords — including passwords for the core network router/firewall, network switches, the corporate VPN, the HR system, email server administration, Windows Active Directory administration, and Windows desktop administration.

That meant that Ed could have held hostage nearly all the company's major business processes, including the corporate website, email, financial reporting system and payroll. "This guy had keys to the kingdom," says Linkous.

So the company and Linkous' firm launched an operation right out of *Mission: Impossible*. They invented a ruse that required Ed to fly overnight to California. The long flight gave Linkous' team a window of about five and a half hours during which Ed couldn't possibly access the system. Working as fast as they could, the team mapped out the network and reset all the passwords. When

Continued on page 22

IBM®

Are you overpaying for Oracle Database?

Hint: you're overpaying for Oracle Database.

The first thing to consider when thinking about DB2® for your business: it's as low as 1/3 the cost of Oracle Database. Then consider DB2 on Power Systems™ with 3x the performance per core of Oracle Database on SPARC, in TPC-C and SAP SD benchmarks. Overall, an ironclad case for IBM. There's more where that came from, too.

ibm.com/facts

COST based on publicly avail U.S. info on 2/10/2011 for IBM DB2 Advanced Enterprise Edition + Oracle software w/comparable capabilities. IBM: 100 Processor Value Units. Oracle: assumes 1.0 processor multiplier. Both incl. Y1 maint/support. PERFORMANCE: www.tpc.org as of 01/26/11 [IBM Power 780 (3 x 64 C)(24 Ch/192 C/768 Th); 10,366,254 tpmC; $1.38/tpmC; avail 10/13/10 v. Oracle SPARC SuperCluster w/T3-4 Servers (27 x 64 C)(108 Ch/1728 C/13824 Th); 30,249,688 tpmC; $1.01/tpmC; avail 6/1/11]. TPC-C is a trademark of Transaction Performance Processing Council. www.sap.com/solutions/benchmark/ as of 01/26/11 [IBM Power 795 (32 P/256 C/1024 Th); 126063 users/2-tier SAP ERP 6.0 pack4/AIX 7.1 + DB2 9.7; cert 2010046 v. Oracle SPARC Enterprise Server M9000 (64 P/256 C/512 Th); 39100 users/2-tier SAP ERP 6.0/Solaris 10, Oracle 10g; cert 2008042]. SAP is a registered trademark of SAP AG in Germany and several other countries. IBM, the IBM logo, ibm.com, DB2, Power Systems, Smarter Planet and the planet icon are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at www.ibm.com/legal/copytrade.shtml.
© International Business Machines Corporation 2011.

Continued from page 20

Ed landed in California, "the COO was there to meet him. He was fired on the spot."

THE COST: Linkous estimates that the incident cost the company a total of $250,000 to $300,000, which includes Sabera's fee, the cost of flying Ed to the West Coast on short notice, the cost of litigation against Ed, the costs associated with hiring a temporary network administrator and a new CIO, and the cost of making all of the company's software licenses legitimate.

PREVENTIVE MEASURES: What could have prevented this disaster? Obviously, at least one other person should have known the passwords. But more significant was the lack of separation of duties. The retailer had a small IT staff (just six employees), so Ed was entrusted with both administrative and security responsibilities. That meant he was monitoring himself.

Separating duties can be a particularly tough challenge for companies with small IT staffs, Linkous acknowledges. He suggests that small companies monitor everything, including logs, network traffic and system configuration changes, and have the results evaluated by someone other than the systems administrator and his direct reports. Most important, he says, is letting IT people know that they are being watched.

Second, the company failed to do a thorough background check when it hired Ed. In CERT's research, 30% of the insiders who committed IT sabotage had a previous arrest. In fact, any kind of false credentials should raise a red flag. Although the company had done a criminal background check on Ed (which was clean), it did not verify the credentials on his résumé, some of which were later found to be fraudulent. (He did not, for example, have the MBA that he claimed to have.)

Third, Ed's personality could have been viewed as a red flag. "He seemed to believe that he was smarter than everyone else in the room," says Linkous, who met Ed face-to-face by posing as an ERP vendor before the sting operation. Ed's arrogance reminded Linkous of the infamous Enron executives. "He was extremely confident, cocky and very dismissive of other people."

CERT has found that rogues often have prickly personalities. "We don't have any cases where, after the fact, people said, 'I can't believe it — he was such a nice guy,' " says Cappelli.

Outsourcing Incenses Employee

"Sally," a systems administrator and a database manager, had been with a Fortune 500 consumer products company for 10 years and was one of its most trusted and capable IT workers, according to Larry Ponemon, founder and chairman of the Ponemon Institute, an IT security research firm.

She was known as a pinch hitter — someone who was able to help solve all kinds of problems. For that reason, she had accumulated many high-level network privileges that went beyond what her job required. "There is this tendency to give these people more privileges than they need because you never know when they'll need to be helping someone else out," says Ponemon.

She sometimes worked from home, taking her laptop, which was configured with those high-level privileges. The company's culture was such that IT stars like Sally were given special treatment, says Ponemon. "The IT people made an end-run around certain policies," he says. "They could decide what tools they wanted on their systems."

But when the corporation decided to outsource most of its IT operations to India, Sally didn't feel so special. Although the company had not yet formally notified the IT staff, says Ponemon, it was obvious to IT insiders that time was running out for most of the department's employees.

Sally wanted revenge. So she planted logic bombs that caused entire racks of servers to crash once she was gone.

At first, the company had no clue what was going on. It switched to its redundant servers, but Sally had planted bombs in those as well. The company had a hard time containing the damage because it didn't follow any apparent rhyme or reason. "A malicious employee [who's] angry can do a lot of damage in a way that's hard to discover immediately and hard to trace later," Ponemon notes.

Eventually, they traced the sabotage to Sally and confronted her. In return for Sally's agreement to help fix the systems, the company did not prosecute her. In addition, Sally had to agree never to talk publicly about the incident. "They didn't want her going on *Oprah* and talking about how she broke the backbone of a Fortune 500 company," says Ponemon.

A Rogue IT Gallery

The threat from trusted insiders is real. IT employees and contractors have been convicted of hacking, planting logic bombs, and stealing money and code.

2011: A software engineer at British Airways was found guilty of using his position to **plan a terrorist attack** on behalf of a Yemen-based radical cleric.

2010: An IT employee at Bank of America pleaded guilty to charges that he **hacked the bank's ATMs** to dispense cash without recording the activity.

2010: A contract programmer who was fired by Fannie Mae was convicted of **planting malicious code** that was set to destroy all data on the organization's nearly 5,000 servers.

2010: A Goldman Sachs programmer was found guilty of **stealing computer code for high-frequency trading** from the investment bank when he left to join a startup.

2010: A Utah computer contractor pleaded guilty to **stealing about $2 million** from four credit unions that he performed IT services for.

2008: A systems administrator at Medco Health Solutions who was worried about layoffs **planted a logic bomb** that would have deleted prescription data from Medco's network.

2006: A systems administrator at UBS PaineWebber who was disgruntled with his pay and bonuses was found guilty of **planting a logic bomb** that affected about 1,000 company computers and caused about $3 million worth of damages.

SOURCE: PRESS REPORTS

THE COST: The estimated total cost to the company: $7 million, which includes $5 million in opportunity costs (downtime, disruption to business and potential loss of customers) and $2 million in fees for forensics and security consultants, among other things.

PREVENTIVE MEASURES: What did the company do wrong? First, the incident is a classic example of "privilege escalation," which is what happens when privileges are granted to an individual to handle a specific task but are not revoked when the person no longer needs them, says Ponemon.

Second, an entitlement culture led to no separation of duties and very little oversight of IT. Because of that, management missed an important red flag. After the incident, the company discovered that Sally had "lost" 11 laptops over the previous three years. The help desk staff was aware of this, but no one ever reported it to management, partly because of Sally's status in the organization. Nobody knows what she did with those laptops; it could be that she was just careless — but "that's a problem in and of itself if you're a systems administrator," Ponemon observes.

Third, given the tense atmosphere created by the outsourcing decision, the company should have been more vigilant and more proactive in monitoring potentially angry employees.

Even if you haven't announced anything to your employees, it's a mistake to think they don't know what's going on, says Ponemon. "The average rank-and-file [worker] knows within a nanosecond of when the CEO signs the [outsourcing] contract," he says. If you aren't already monitoring your IT people, now is the time to start. For best results, kick off the program with a very public pronouncement that you are now monitoring the staff.

According to CERT, many cases of sabotage are the result of a disgruntled employee committing an act of revenge. And such acts can happen in the blink of an eye, as the next story illustrates.

A Firing Gone Wrong

When this Fortune 100 company upgraded its security, it made a nasty discovery. One of its senior system admins, who had been there at least eight years, had surreptitiously added a page to the company's e-commerce website. If you typed in the company URL followed by a certain string of characters, you got to a page where this admin, whom we'll call "Phil," was doing a brisk business selling pirated satellite TV equipment, primarily from China, according to Jon Heimerl, director of strategic security at Solutionary, a managed security services provider hired to address the problem.

The good news: Improved security caught the perpetrator. The bad news: Management botched the firing process, giving him an opportunity to take a parting shot.

Itself a retailer in high-tech equipment, the company wanted to get rid of Phil and his website as quickly as possible because it feared lawsuits from satellite equipment manufacturers. But while Phil's manager and security staffers were on their way to his office, a human resources representative called Phil and told him to stay put. Heimerl isn't sure exactly what the HR person said, but it was apparently enough for Phil to guess that the jig was up.

> **We're trying to figure out how to get the message to the C-level people that this is not just an IT problem.**
>
> **DAWN CAPPELLI,** TECHNICAL MANAGER, CERT INSIDER THREAT CENTER

Already logged in to the corporate network, he immediately deleted the corporate encryption key ring. "As he was hitting the Delete key, security and his manager showed up and said, 'Stop what you're doing right now, and step away from the terminal,' " according to Heimerl. But it was too late.

The file held all the encryption keys for the company, including the escrow key — a master key that allows the company to decrypt any file of any employee. Most employees kept their own encryption keys on their local systems. However, the key ring held the only copies of encryption keys for about 25 employees — most of whom worked in the legal and contracts departments — and the only copy of the corporate encryption key. That meant that anything those employees had encrypted in the three years since they had started using the encryption system was permanently indecipherable — and thus virtually lost to them.

THE COST: Heimerl hasn't calculated how much money the incident cost the company, but he estimates that the loss of the key ring file amounted to about 18 person-years of lost productivity — a figure that takes into account both the work that went into creating files that are now permanently encrypted and the time devoted to re-creating materials from drafts, old emails and other unencrypted documents.

PREVENTIVE MEASURES: Focusing only on what happened after they discovered the rogue website, the company made two crucial mistakes, says Heimerl. It should have shut down Phil's access immediately upon discovering his activities. But managers also left themselves vulnerable by not keeping a secure backup of critical corporate information. (Ironically, the company thought the key ring was so sensitive that no copies should be made.)

The Best Defense Is Multifaceted

The overall lesson from these horror stories is that no single thing can protect you from rogue IT people. You might have great technical security — like the multitiered security system that ultimately detected Phil's unauthorized website — and yet a simple mistake by HR can lead to disaster. Or there could be big red flags in terms of behavior or personality that go unnoticed — like Sally's missing laptops.

It's a combination of technical safeguards and human observation that offers the best protection, says CERT's Cappelli.

And yet it's hard to convince companies to do both. Executives tend to think such problems can be solved with technology alone, at least partly because they hear vendors of monitoring systems and other security products claiming that their tools offer protection. "We're trying to figure out how to get the message to the C-level people that this is not just an IT problem," Cappelli says.

It's a difficult message to hear, and a lesson that many companies only learn the hard way. Even if more companies were forthcoming with the details of their horror stories, most CEOs would still think it could never happen to them. Until it did. ◆

Harbert *is a Washington, D.C.-based writer specializing in technology, business and public policy. She can be contacted through her website, TamHarbert.com.*

Legal Risks IN THE Cloud

Don't sign that contract until you consider **five red flags** in cloud service deals.

BY STACY COLLETT

LAST YEAR, a global food manufacturing and distribution company set out to move its HR talent management processes to a software-as-a-service provider. But as attorneys for the food company reviewed the proposed contract, they found some potentially serious legal land mines.

For starters, the SaaS provider had operations in the U.S., Europe and Canada. "Europe and Canada are two jurisdictions that heavily regulate [the use of] personal information. Since this was an HR system, there would be a lot of personal information," recalls Rebecca Eisner, an attorney specializing in outsourcing who represented the food company.

The provider also wanted the flexibility to move the company's information to data centers anywhere in the world, and that would subject the company to the laws of whatever country the data passed through or landed in.

But there was no turning back. The company was as smitten with the SaaS application as it was unaware of the legal risks. After two months of negotiations, the two sides agreed on a contract.

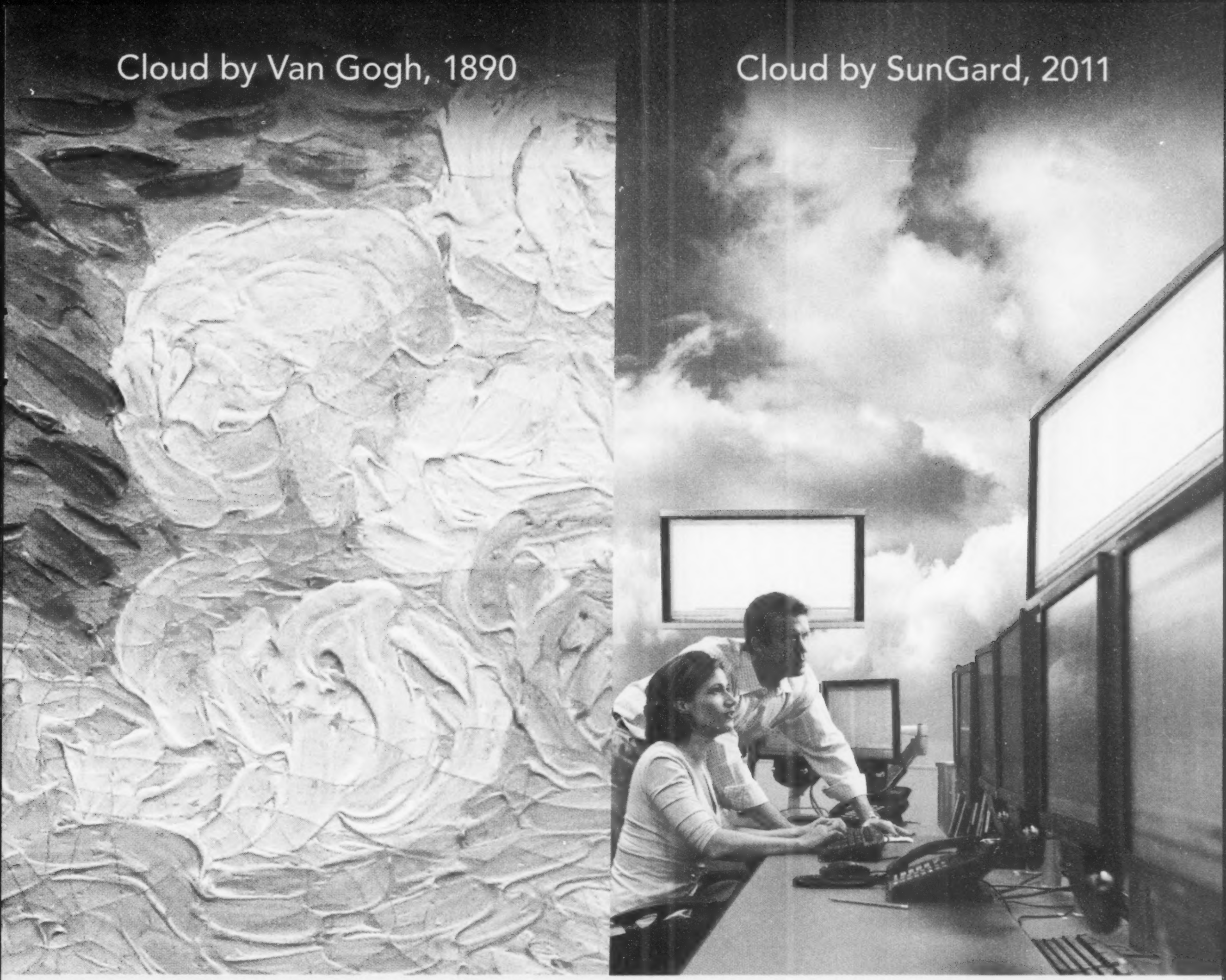
"The [SaaS provider] didn't want to admit their lack of sophistication on these issues. But they understood where we were coming from," says Eisner, a partner in the Chicago office of the law firm Mayer Brown. "Ultimately, they understood that if they were going to get [the food company] as a customer — and other global companies in the future — they needed to provide these kinds of minimum protections. So they went along with it."

If you're operating in the cloud or plan to move there soon, here are five areas of legal risk that you shouldn't ignore.

Continued on page 26

Rebecca Eisner

PHOTO ILLUSTRATION BY GETTY IMAGES



A work of art in secure computing.

Building a better cloud takes a revolutionary approach to virtualization that goes far beyond conventional solutions. With a resilient infrastructure and robust security, SunGard provides maximum protection and a fully managed solution that virtually eliminates the risk of failure. Navigate the cloud with confidence as it dynamically scales to meet your needs. With leading-edge technology and a staff of accomplished professionals, SunGard can help make your next cloud computing project a work of art.

Download the white paper
"Building a Better Cloud"
at: sungardas.com/cloud11

© 2010 SunGard. SunGard and the SunGard logo are trademarks or registered trademarks of SunGard Data Systems Inc. or its subsidiaries in the U.S. and other countries. All other trade names are trademarks or registered trademarks of their respective holders.

SUNGARD AVAILABILITY SERVICES

Continued from page 24

1

Privacy

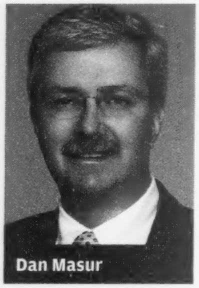
The Health Insurance Portability and Accountability Act (HIPAA) requires companies that disclose personal health information to third parties to enter into "business associate agreements." These contracts stipulate how the third parties should handle such data. "A lot of people don't think of that requirement when they're doing cloud computing — they don't think of it as 'disclosing information' to a third party, but in fact it is," says Polly Dinkel, an attorney at Sideman & Bancroft in San Francisco.

Similarly, the Gramm-Leach-Bliley Act requires financial institutions to enter into contracts with third parties with whom they share their customers' personal information, in order to ensure that the third party stores the data securely. "There has to be a contractual requirement to implement and maintain that kind of safeguard," Dinkel adds.

Executives of financial institutions can be held personally liable for failure to meet those requirements in cloud deals, she says.

The tricky part is knowing exactly where all the cloud providers' data centers and subcontractors are located, says attorney Dan Masur, a partner at Mayer Brown. He says the Sarbanes-Oxley Act requires the original owners of the data to know where the data is and maintain control of it in the cloud.

As Masur puts it: "You have data moving all over the world to wherever [the cloud provider] has capacity. It's not just the provider, but a whole web of subproviders and subcontractors and platforms. Where exactly is it at any moment in time? How many countries is it hitting and thereby [subject to] the laws of those countries? Even if you have a contract in place with the provider, can you really be sure they have flow-down clauses that apply the contract terms to this web of subcontractors?"


Dan Masur

Customers need to insist that the subcontractors be identified and that contract terms apply — or "flow down" — to them, Masur says. The good news is that some major cloud providers will offer U.S.-only public clouds, as well as assurances that the relevant terms of the contract have been applied to subcontractors.

At Schumacher Group, a Lafayette, La.-based healthcare company, about 80% to 90% of IT processes are hosted in the cloud through 12 different service providers.

"All of the vendors we select must have HIPAA policies and compliance in place," says CIO Douglas Menefee. He also requires cloud providers to sign a business associate agreement that says vendor employees can only look at information that is relevant to their jobs, and only when necessary.

2

Cross-Jurisdiction Compliance

Gartner's Global IT Council for Cloud Services — a group of CIOs trying to hammer out standard ways of working in the cloud — complains that "service providers have not done a good job of explaining which jurisdictions they put data in and what legal requirements the service consumer must therefore meet."

Contract Clinchers

Avoid legal risks in the cloud by drawing up a contract that does the following:

- Requires the service provider to notify you if it receives a **search warrant or subpoena** for information.
- Spells out the **security controls** and states where the data will be stored.
- Specifies how quickly the service provider will respond to **e-discovery requests**, and ensures that the information can be easily retrieved.
- Requires the service provider to notify you when it **hires a new subcontractor or moves data** to a new jurisdiction.
- Provides an **exit clause** that protects you if the deal doesn't work out or the service provider goes out of business. This clause should ensure that you can get your data back in a specified format within a specified period of time.

– STACY COLLETT

The group's manifesto says cloud customers have "the right to understand the legal requirements of jurisdictions in which the provider operates." Otherwise, if the cloud provider stores or transports the customer's data in a foreign country, "the consumer becomes subject to laws and regulations it may not know anything about," the council says.

For example, the European Union has some of the strictest privacy laws in the world — and complying with those laws gets more complicated in the cloud.

Transferring data out of the EU is prohibited unless the EU deems that the receiving country has "an adequate level of protection" — and very few countries meet that requirement, says Dinkel. "That's definitely a concern if you have servers in this country with data related to an EU person and are moving the data from one server to another," she says. "Some providers have segregated clouds for EU data to get around this problem."

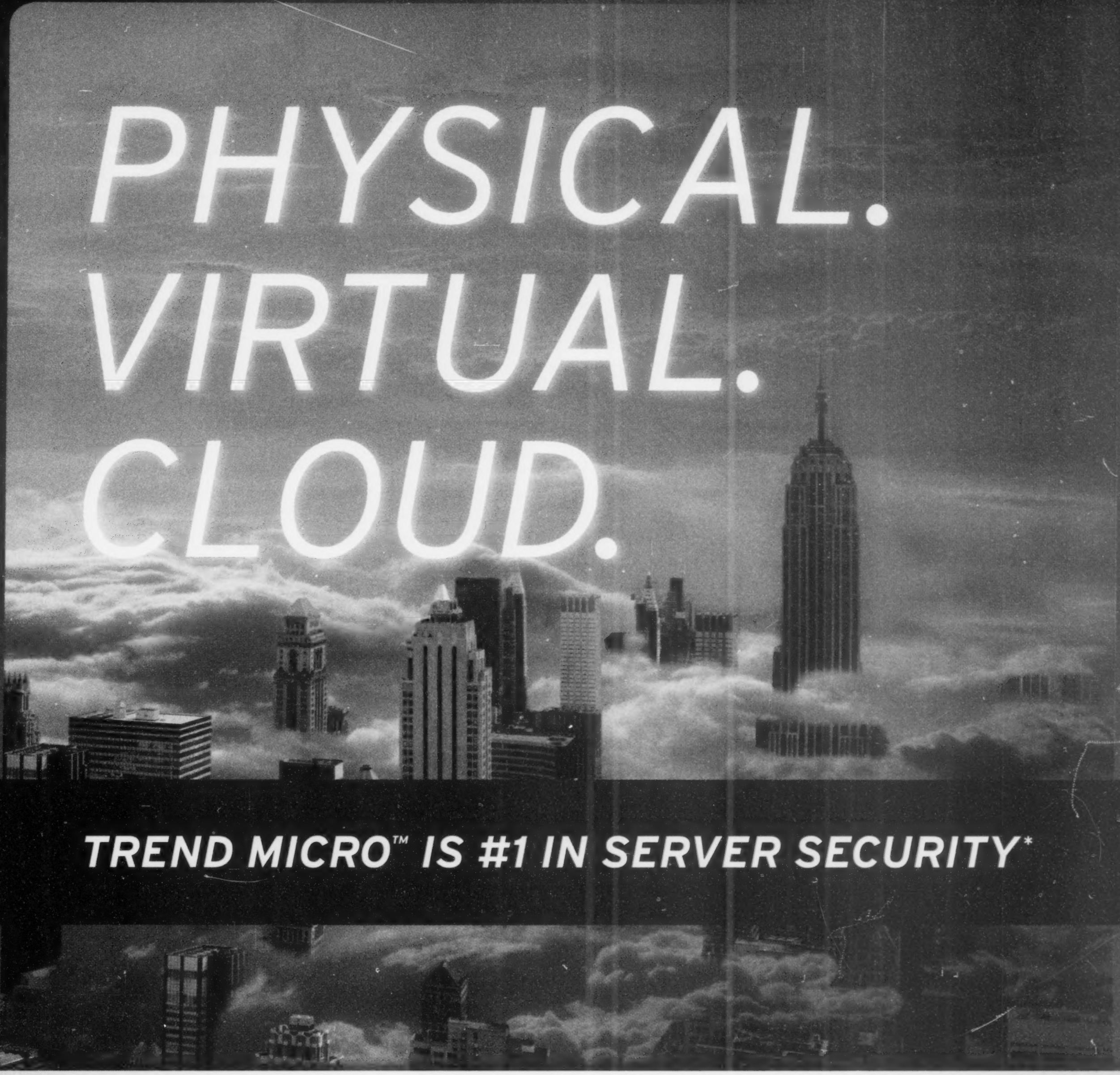
European regulators are now examining cloud computing to try to figure out how the new technology fits its existing framework for regulating the use, collection, storage and transfer of personal data. Dinkel says cloud computing users can expect to jump through extra hoops. For example, they may have to obtain special approvals and file reports with European data protection authorities detailing plans for the use and storage of data.

Cloud users should also know that the location of the provider or its servers could determine where a lawsuit would be brought if a problem arose. "You may find yourself defending an action in another state or another country, depending on where your provider is located," Dinkel says.

Polly Dinkel

Schumacher Group's cloud contracts require that data be stored at centers inside the U.S. "It doesn't make sense for them to store our data overseas," Menefee says.

Continued on page 28



Trend Micro provides unmatched protection for servers wherever they are. According to IDC, a global authority on technology market trends, more companies use Trend Micro server security than any other. Add to that our breakthrough key management and encryption solution for both public and private clouds, and optimized protection for virtualized datacenters, and it's easy to see that Trend Micro is more than just great security. We're a business advantage.

TREND MICRO™

Securing Your Journey to the Cloud

» LEARN MORE AT TRENDMICRO.COM/CLOUD

Read the latest on cloud security.

*IDC, *Worldwide Endpoint Security 2010-2014 Forecast*

© 2011 Trend Micro, Inc. All rights reserved. Trend Micro and the t-ball logo are trademarks or registered trademarks of Trend Micro, Inc.

Continued from page 26

3 Search Warrants

One of the scary features of public clouds is that data from multiple customers may be kept on the same server, says Dinkel. "If the provider gets served by a warrant with regard to one customer, and a number of other customers' data happens to be on the same server, all that data could be seized and become inaccessible to the company that was not the intended target of the search," she explains.

Commingling of data was a serious problem in 2009, when the FBI raided two data centers in Texas as part of an investigation involving a specific data center customer. FBI agents seized about 220 servers, as well as routers, switches, server cabinets and even power strips. Press reports indicated that the seizure resulted in millions of dollars in lost revenue for the data center. It also put many of the data center's customers out of business or at risk of closure, according to reports.

How do you mitigate such risks? A private cloud can certainly eliminate commingling. If that's not an option, get assurances from the cloud service provider regarding how customer data is partitioned, so that a search warrant and seizure doesn't affect your data.

4 E-discovery

A data owner who is sued has an obligation to preserve any information that's relevant to the litigation and to collect it for legal discovery purposes. The requirement to preserve data applies if the data is in your "custody, control or possession." And for cloud customers who own data, "it's pretty clear at this point that if it's in the cloud, it's still considered to be in your custody, control or possession," says Dinkel. So if the vendor doesn't preserve it or can't produce data before the discovery deadline, then the cloud user "can be sanctioned for that," she says.

Did You Know?

- The European Commission is in the process of updating (i.e., strengthening) the **1995 EU Data Protection Directive**.
- **Mexico has adopted a broad federal privacy law** that will affect many large U.S.-based companies operating in that country.
- In the U.S., **it's easier to subpoena or otherwise compel the release of information when it's held by a third party** (such as a cloud provider) than when it's held by the company that originally collected the data.
- The Patriot Act, in some circumstances, allows the U.S. government to obtain personal information held by a cloud provider **without the knowledge of the data collector** or the subject being investigated.

SOURCE: "PRIVACY TRENDS 2011," ERNST & YOUNG, JANUARY 2011

> **"If there is a breach, it's [the cloud service provider's] responsibility, not ours.**
>
> **DOUGLAS MENEFEE,** CIO,
> SCHUMACHER GROUP

What's more, the opposing party can go directly to the cloud provider to find relevant records. "The data owner loses control of the situation at that point," Dinkel says.

Complicating matters further, cloud providers have different storage procedures, and if data isn't mapped properly, retrieving it could be difficult and expensive.

When an e-discovery request lands at your door, you must be able to produce documents in a timely manner. If you can't, you could face heavy fines (in one case, the proposed fine was $50,000 per day). What's more, companies may have to go back three to five years for relevant data because cases can take years to reach the courts.

Big cloud providers are aware of the need for prompt action on e-discovery requests, and they're often able to track and retrieve data quickly by maintaining the original metadata attached to the records.

Lawyers say cloud contracts should require vendors to maintain metadata for easy retrieval and compel them to meet deadlines for producing electronic documents when requested.

5 Data Security

Methods for protecting data in the cloud, such as encryption, are well documented. But there are also risks associated with having all of a company's records in one location, where they would provide hackers with a tempting smorgasbord of information. Some cloud providers are already addressing that risk.

The security model for Google Apps, for instance, allows stored data to be separated at the bit level and distributed to multiple sites across the country. "We found that intriguing," says Menefee, a Google Apps user. "If they had a breach, the [hacker] would only have components, pieces of a giant puzzle."

Another question: Who pays for costs associated with a security breach in the cloud? "You want [the service provider] to be paying for it — because it may be something on their end that caused the breach," says Dinkel.

In many states, an organization that's storing customer data in a public cloud is responsible for notifying its customers in the event of a data breach at the cloud vendor. "But you may not know in a timely fashion if there's been a breach," unless timely notification is required in the contract, she says.

Menefee includes security-related clauses like that in all of Schumacher Group's cloud contracts. "If there is a breach, it's their responsibility, not ours," he says.

Risks are always changing, and it's important to consult with legal counsel when contracts are up for renewal to make sure new issues are addressed. For example, Menefee plans to add exit clauses to future contracts to protect Schumacher Group if a provider undergoes a change of ownership.

"That was kind of an 'Aha!' moment in the past six months. There's going to be a huge consolidation, I believe, inside the cloud marketplace. I'm looking for the ability to exit out of contracts" if there's a change in ownership or a service provider fails to meet the service-level agreement during a changeover, Menefee says. "For me, it's going to become part of our standard governance." ◆

Collett *is a* Computerworld *contributing writer. You can contact her at stcollett@aol.com.*

beyond
silos
together.

it's agile, yet efficient.
intelligent, yet simple.
virtual, yet real.

it's servers, networking, storage
and virtualization. together.
so you can allocate resources
and deliver services.
on demand. on time. every time.

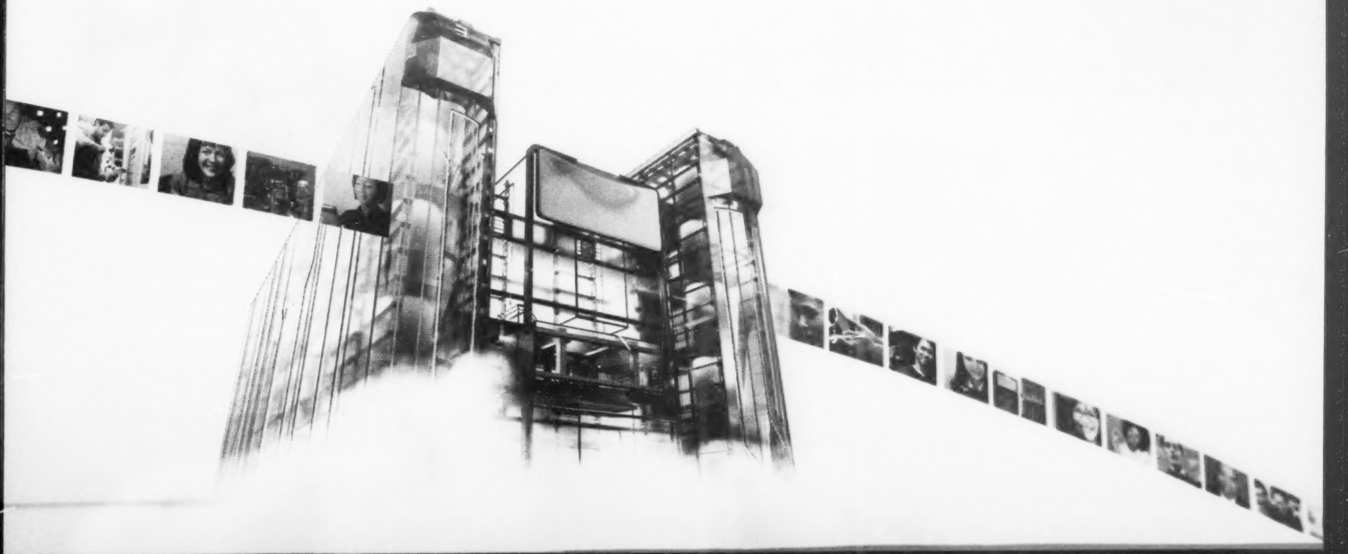
bring big ideas to life
by transforming silos into new ways
to collaborate and innovate.

introducing the Cisco data center
business advantage.

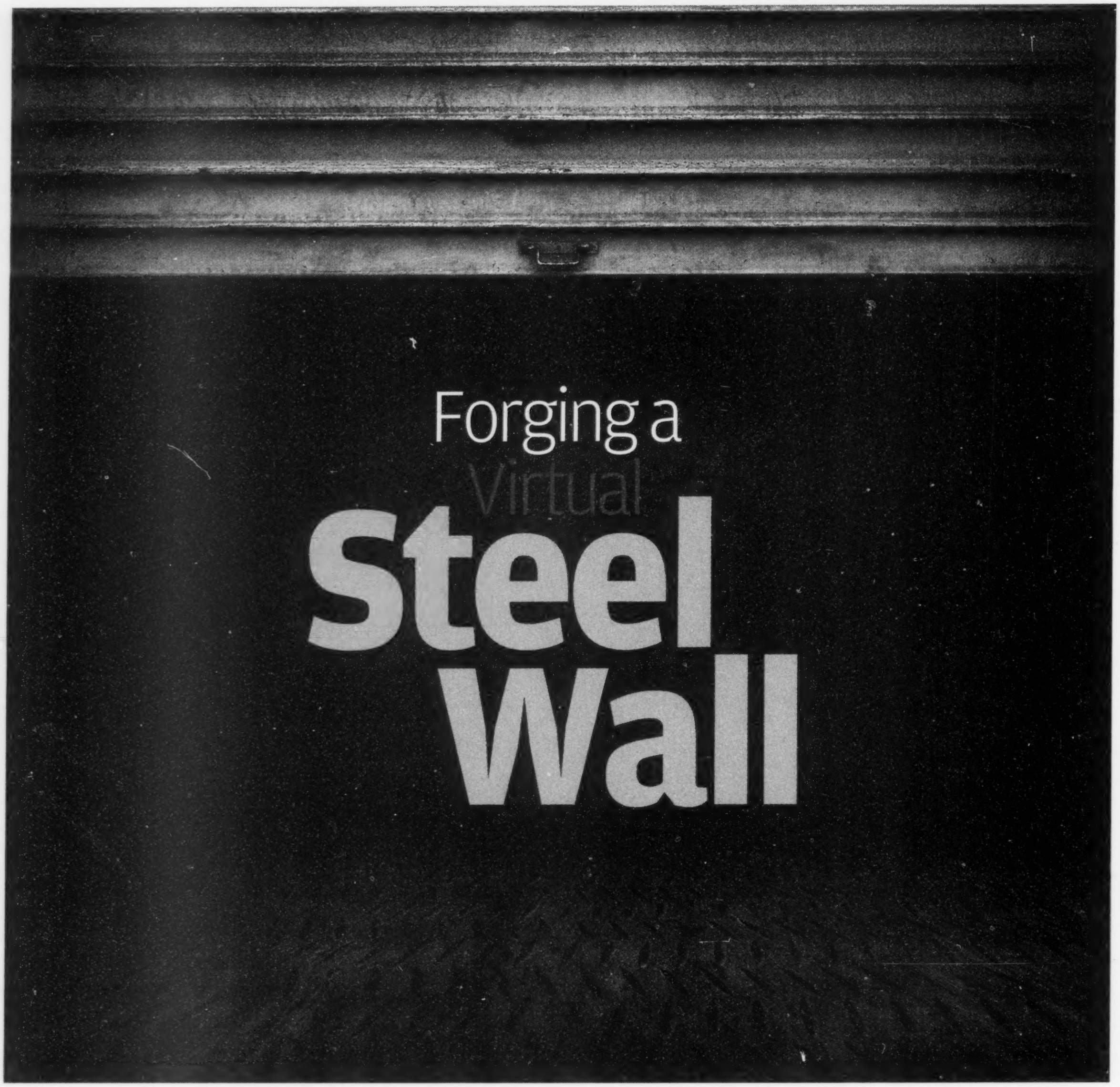
cisco.com/go/dcbusiness

together we are
the human network.

CISCO.



©2011 Cisco Systems, Inc. All rights reserved.



Forging a Virtual Steel Wall

Hardening software to prevent security breaches is coming back into fashion. And, yes, it's worth the trouble.

BY JOHN EDWARDS

GLENN PHILLIPS, president of Pelham, Ala.-based Forté, says that the dedicated Windows workstations his company sells to hospital emergency room administrators must not only be secure, but absolutely tamperproof as well. After all, lives depend on the machines' flawless operation.

Forté's applications show emergency medical technicians the emergency room's current availability status, "so our software must be the program that is always running," Phillips says. "We cannot have anyone closing our program, adding games, changing Windows settings and so on."

Phillips and others who need to create highly secure workstations or servers are turning to hardening to create a virtual steel

© FOTOLIA / PHASE4PHOTOGRAPHY

wall against intruders. The hardening process involves removing nonessential tools and utilities from an operating system or application, any of which could be used to help an attacker gain unauthorized access to system settings or data.

The approach can be used to substitute for or, more commonly, complement other security practices and technologies, such as network firewalls.

Hardening is a technique that's been around since the earliest days of networked computers, but it gradually fell into disuse as software vendors boosted the security of their products and IT managers adopted new security technologies and practices.

Even so, the security improvements haven't made hardening any less practical or useful. "It's still one of the least expensive and most effective ways of protecting yourself or preventing infections or outages," says Chris Rafter, vice president of consulting services at Logicalis Group, a systems integrator in Bloomfield Hills, Mich.

Peter Makohon, a senior security and privacy manager at the New York office of professional services firm Deloitte & Touche, says hardening is coming back into fashion as more enterprises face pressure to patch every possible security hole that could conceivably be exploited as a pathway into a corporate system. Regulatory compliance is another factor that's inspiring many enterprises, particularly those in highly regulated industries, to take another look at hardening.

Just about any enterprise can benefit from hardening, Rafter says. "Operating systems and applications are definitely a lot more secure than they were a long time ago, but there's still logic to turning off unnecessary services and basically only activating and using what you really need," he contends. "Plus, it doesn't require a great deal of effort."

Most vendors long ago dropped any objections to customers hardening their products. Many — including Microsoft — actively encourage the practice. "Hardening an operating system is a key step in protecting a system from intrusion," says Chase Carpenter, a manager in Microsoft's Windows Server unit.

Carpenter says enterprise hardening efforts have traditionally covered the client and server operating systems, but with attacks increasingly targeting the application layer, the focus of hardening is shifting to applications. Microsoft views its Security Compliance Manager and Security Baseline products as hardening tools.

Manual or Automatic?

While most user organizations opt to handle the hardening work themselves — assigning the task to either IT staffers or outside consultants — some have opted to use commercial software that's designed to automate the process. For example, CellTrust, a mobile applications developer in Scottsdale, Ariz., hardened its servers and its Linux-based network appliances with a product called Security Blanket from Raytheon Trusted Computer Solutions, based in Herndon, Va.

Vahid Sedghi, CellTrust's vice president of technical services, says that the decision to go with a hardening product came down to convenience and a desire not to take IT staffers away from their core responsibilities. "It was either having our Linux folks go manually out there and see what has been applied and what hasn't been applied in our environment, or letting this tool to do the work in a more automated fashion," he explains. Sedghi says that a process that previously involved hours of writing, pushing and applying Linux scripts was eventually whittled down so it now takes less than 60 minutes.

Sedghi feels that hardening provides a valuable extra layer of protection. "From a business perspective, it lowers the risk of downtime," he observes.

Hardening complements his business's other security measures, Sedghi says, noting that "obviously, we have our different vulnerability scanning tools and network security tools in place." Standard security tools are still important, he notes, because they perform tasks that hardening doesn't address. "They protect, monitor and scan our network and servers," he says. "Hardening just closes the gaps."

Getting It Right

Knowing exactly what to keep or delete among the various operating system or application tools and features is the biggest challenge facing users undertaking hardening projects for the first time. Organizations that decide to do the work in-house need to commit to a process of gathering information about best practices, says Makohon.

He notes that operating system and application vendors, as well as open-source organizations, are usually willing to offer some guidance to enterprises embarking on hardening projects. Software- and security-oriented Web forums are also good sources of practical information about hardening.

Hardening: **The Basics**

Chase Carpenter, a manager in Microsoft's Windows Server unit, says a hardening strategy should focus on the following tactics:

Reducing the attack surface

- Remove nonessential tools and features.
- Disable unnecessary services and protocols.
- Remove or secure file shares.

Restricting user access

- Limit the number of user accounts.
- Curb access rights.

Protecting against known and theoretical attacks

- Configure common security settings.
- Apply necessary patches and updates.
- Use encryption where possible to protect critical data.

Using available tools to detect attacks

- Configure the system to log appropriate and inappropriate user access.
- Configure the system to make it difficult or impossible for attackers to cover their tracks.

– JOHN EDWARDS

> **Just remember, the goal is hardening, not making things harder to use.**
>
> **PETER MAKOHON,** SENIOR SECURITY AND PRIVACY MANAGER, DELOITTE & TOUCHE

There are many resources, both in the private and public sectors, that help define baseline security configuration settings, says Makohon. They also offer information about how certain configuration settings should be made, the order in which they should be made, and what the resulting state of operation should be.

Phillips says that learning how to harden Windows on the Dell OptiPlex desktops that Forté markets to emergency room operators wasn't particularly difficult. "Almost everything we did, we found on the Web," he says. "There were a few things we found through trial and error, such as when we weren't sure how something would work, or when the instructions [found on the Web] weren't very good, but most things you can pretty much find yourself."

Veterans of this process recommend working closely with the application maintenance or application development team at the outset, to make sure you don't turn off something that is essential now or will be needed in a system you're planning to build later.

Makohon also advises enterprises to check with their software's developer to ensure that they're using the most up-to-date version of the product they're planning to harden. "It doesn't make sense to tackle hardening tasks that the vendor may have already addressed," he says.

» GLENN PHILLIPS says Forté hardens the PCs it sells for use in emergency rooms because they must be absolutely tamperproof.

Rafter says that successful hardening requires a holistic approach that takes overall system security, performance, usability and other key factors into consideration. "It's important to perform a very thorough asset inventory and to make sure that you've covered all the potential entry points, or places where malware could be executed," he says.

While Phillips thinks of hardening as a "foolproof" means of securing systems, he adds that the technique shouldn't be used as an excuse to skimp on or ignore traditional security measures. "Hardening needs to be viewed as an 'extra,' not as an 'instead of,' " he says.

Don't Forget Training and Testing

Training is often neglected, but it should be a key part of the hardening process. Why? Because users may work very hard to circumvent hardening-created safeguards that just seem inconvenient; they need to understand why the safeguards are there.

"You still have to train your users in everyday security practices — what to do and not to do — because no matter what you've done to lock down [the operating system or application], within a few months there will be something out there that can bypass that. It's a moving target," Phillips says. He notes that a certain amount of rehardening is inevitable over time.

Phillips recalls a security hole that surfaced with the arrival of USB memory sticks. "We had done all this hardening, and then we discovered that you could simply take a USB drive, plug it into the USB slot, and [a window] would pop up asking, 'Do you want to run this?' "

The discovery prompted a fast repair job to modify the operating system's permissions settings. "We think our hardening solution was far more elegant than taking a hot-glue gun and filling up all the USB ports," Phillips says.

The final step in hardening is testing. "Anytime security configuration changes are made, they can have an impact on manageability, usability or application compatibility," Carpenter says.

Makohon agrees. "It's important to test platform configurations not only from a functionality standpoint, but from a performance and availability standpoint after they've been hardened," he says.

All tests need to be conducted under real-world conditions. "If systems have been hardened in a test environment, can they be properly managed and accessed?" Makohon asks. "It's one thing if they can still perform their primary function, but now can you still gain the required information in order to see how they're performing, or to see what types of logs they are writing, or have [the systems] available to help further track the presence of a malicious insider or a cybercriminal?"

Phillips advises managers to do a thorough job and make sure features are removed, not just made inactive. There's a big difference between removing a feature or command and simply locking it. "If something is simply not there, users are less likely to get frustrated, as opposed to seeing a visible option that won't work," Phillips adds. There's also the possibility that an attacker could exploit a dormant feature.

However, Phillips warns managers striving for maximum protection not to harden their software to the extent that it cripples functionality. "You want some things to be restrictive, [but] the tools need to be supportive and flexible to accomplish business goals," he says. "This is something that I see IT mess up over and over again."

Makohon agrees. "Just remember," he says, "the goal is hardening, not making things harder to use." ◆

Edwards *is a technology writer in the Phoenix area. You can contact him at jedwards@gojohnedwards.com.*

SNW SNIA COMPUTERWORLD BEST PRACTICES AWARDS PROGRAM

SNW, in conjunction with *Computerworld* and the Storage Networking Industry Association (SNIA), proudly announce the results of the SNW "Best Practices" Awards. Winners were honored at a ceremony during SNW Spring 2011.

Congratulations TO THE 2011 WINNERS

Best Practices in Adopting Emerging and Innovative Technologies

WINNER

California Emergency Management Agency (Cal EMA) | Mather, California

FINALISTS

District of Columbia Water and Sewer Authority (DC Water) | Washington, DC

International Justice Mission | Arlington, Virginia

Rockford Construction | Grand Rapids, Michigan

U.S. Customs & Border Protection, Office of Information and Technology | Springfield, Virginia

Best Practices in IT Consolidation, IT Efficiency and Data Center Design

WINNER

The E.W. Scripps Company | Cincinnati, Ohio

FINALISTS

The Chinese University of Hong Kong | Hong Kong, China

Department of Innovation, Industry, Science and Research (DIISR) | South Melbourne, Australia

O.C. Tanner Company | Salt Lake City, Utah

Reliance Communications Ltd. | Maharashtra, India

Best Practices in Storage Resiliency, Data Protection and Recovery

WINNER

Cloudmark | San Francisco, California

FINALISTS

Arnold Worldwide | Boston, Massachusetts

Escondido Union High School District | Escondido, California

Farm Credit Services of Mid-America | Louisville, Kentucky

FICO | St. Paul, Minnesota

Best Practices in Virtualization and Cloud Computing

WINNER

Bloomington School District #87 | Bloomington, Illinois

FINALISTS

The Aura Group | Fullerton, California

High Moon Studios | Carlsbad, California

Patients First Health Care | Washington, Missouri

United Way of Atlanta | Atlanta, Georgia

The SNW Spring 2011
Best Practices Awards Program
Sponsored by

FUSION-iO

THANK YOU TO OUR SNW SPRING 2011 JUDGES:

Wendy Betts | Northern Trust
Brian Carlson | *CIO* magazine
Noemi Grezydorf | IDC
Derek Hulitzky | IDG Enterprise
Lucas Mearian | *Computerworld*
David Stevens | Carnegie Mellon University
Terry Yoshii | Intel Corporation

Security Manager's Journal

MATHIAS THURMAN

Trouble Ticket

» **At issue:** A third party's software code unleashed malware.

» **Action plan:** Look at the entire software development process and incorporate automated checks of source code.

Keeping Our Code Safe

Our manager's company has shockingly little oversight on the security of software code written for it by third parties.

WE HAVE a major problem, which explains why I'm sitting in an airport right now. I'm heading off to visit some third parties that develop portions of our software for us.

The problem is that some software we recently developed in-house was infected with malware, and the source of that malware was traced back to a third party's code. We were fortunate that the malware was pretty well contained, but the fact that this could happen at all raises questions about the security of our methods.

After I heard about this incident, I started looking into my company's software development life-cycle (SDLC) process, which is meant to help us develop systems in a very deliberate and structured manner. To my mind, any SDLC that doesn't include taking sanity checks on security isn't worth much. And upon investigation, it was painfully obvious that we lacked robust security sanity checks for third-party code. Apparently, assumptions were made and we ended up with verbiage in our contracts that said it would be the third party's responsibility to verify that all code was free of security bugs and other potentially threatening anomalies. Assumptions about security always make me wince

In my meetings, I want decisions made on roles and responsibilities, expectations and methodology. Of course, I don't expect developers or quality assurance engineers to manually review source code, so I expect to invest in technology that will help in this analysis.

As I prepared for this trip, I started looking into the technologies that are available in the marketplace for this sort of automated code vetting, and my initial investigation has revealed that several companies offer such tools. There are products that would reside in-house, or we could go with a software-as-a-service option. At this early stage, I find the SaaS model intriguing, since my company has a Web-based collaboration tool that allows third parties to submit code for incorporation into our homegrown software.

JOIN IN the discussions about security! **computerworld.com/blogs/security**

One question we will have to answer is whether we want to burden the third parties with the responsibility of doing the analysis or conduct the analysis ourselves. Burdening the third parties may hinder innovation. Doing it ourselves will add to our overhead.

Dynamic or Static

My research also taught me about the approaches that are available for code checking. There are two principle ways of doing this: static and dynamic. With static analysis, the raw source code is reviewed for indications of poor programming practices that could lead to a security incident, such as leaving sensitive information in the comments of the code; not conducting bounds checks, which can result in buffer overflow attacks; and lack of input validation, which may lead to SQL injection attacks. Dynamic analysis is more, well, dynamic. In a dynamic analysis, you actually attack the compiled application and look for indications that it's susceptible to exploitation.

One constraint for us is that we'll have to find a product that maps to all the programming languages we use; we don't want to have to invest in multiple products to cover everything. And we'll have to review the license model, the support structure, the reporting mechanism and overall flexibility when it comes to incorporating the product into our various SDLC processes. In addition, I'll want the ability to audit and govern the process if necessary.

After my travels, and no doubt a lot more meetings, I'll formulate business requirements and draw up process documents. I don't imagine this will be an overnight change, but given the risks, there will most definitely be a change. ◆

This week's journal is written by a real security manager, **"Mathias Thurman,"** *whose name and employer have been disguised for obvious reasons. Contact him at mathias_thurman@yahoo.com.*

> **"Apparently, assumptions were made about third-party code. Assumptions about security always make me wince.**

TECH
BRIEFCASE

Search, store, and share
IT white papers from across the web.

Search thousands of relevant IT white papers.

Organize what you find by tag or project.

Store and access them from your phone or desktop.

Share your briefcase content with colleagues and friends.

3G
9:41 AM
New
What's Hot
Recommended
Featured
Mitigate Business Risks for Complex Assets through Smarter Maintenance

Optimize Your Linux Experience with Virtualization

Process Center of Excellence

Proven Practices for Upgrading and Migrating to SharePoint Server 2010

Realizing the Benefits from Accounts Payable Optimization in SAP

Download the Tech Briefcase app from the iTunes App Store.

Available on the App Store

OPINION

PAUL GLEN

The Three Ways Users Experience IT

As technology has pervaded the enterprise, the number of ways in which we interact with our consumers has expanded.

THE QUALITY of business relationships is based on much more than the quality of the products and services we deliver. If we're going to improve the relationship between IT groups and the people who consume our technology, we're going to have to start thinking more carefully about their experience of us as well.

As engineers, we tend to believe that the quality of our products should speak for itself, but this never really works out too well. First, we are not merely technology providers. The experience of working with us is part of our value. Second, the consumers of our products can't really directly determine the quality of our products. If they knew enough to judge the technology, they probably wouldn't need us at all — they'd be experts themselves. So they judge by the quality of the experience they have working with us.

But there is no single experience of working with us. As technology has pervaded almost every area of our enterprises, the number of ways in which we interact with our consumers has expanded significantly. There are three dominant types of experiences that IT consumers have, each with different expectations and perceived values.

Daily operations. Business functions like finance, marketing and logistics have incorporated technology into virtually every aspect of their work. The systems we have purchased, customized and written enable them to meet their daily objectives. And most of the people working in those functions live in front of screens as much as we do.

Every day, even when things are going perfectly, they experience our technology and have feelings about how it affects them. Sometimes that technology feels like a tool that enables them; at other times, it feels like an obstacle constraining them.

But when something stops working, they feel frustrated. And when they contact us for support, they are already upset. How we handle their emotions at that moment colors how they think of us in every circumstance.

So how we handle support affects how they feel about us generally.

Operational adaptation. Beyond everyday work, IT consumers want us to help them improve their operations. Whether they are trying to increase efficiency, consolidate functions or adapt to new processes, they need to change how the daily operations use technology.

We help them adapt through projects. The goal of nearly every project is operational change, and the experience of working with us on prioritizing, planning and implementing these changes is distinct from their experience of daily operations.

Strategic change. In the past, business functions didn't really think about IT when considering strategic transformation. We were included only as an implementation afterthought. But as business models have become more dependent on technology as a fundamental enabler, we have (or should have) become central to strategic planning.

The expectations of how we participate strategically are quite distinct from operations or adaptation. But how our consumers feel about our services at lower levels colors how they feel about us at higher levels. It's not uncommon for consumers to wonder, "If they can't fix my laptop, how can they contribute to strategic planning?"

To improve our relationships with our consumers, we need to understand the context of the value we are offering and the expectations that come with that type of value. ◆

Paul Glen is a consultant who helps technical organizations improve productivity through leadership, and the author of the award-winning book *Leading Geeks* (Jossey-Bass, 2003). You can contact him at info@paulglen.com.

dtSearch®

The Smart Choice for Text Retrieval® since 1991

Instantly Search Terabytes of Text

- Desktop with Spider
- Network with Spider
- Publish (portable media)
- Web with Spider
- Engine for Win & .NET
- Engine for Linux

Ask about fully-functional evaluations!

Highlights hits in a wide range of data, using dtSearch's *own* file parsers and converters

- Supports MS Office through 2010 (Word, Excel, PowerPoint, Access), OpenOffice, ZIP, HTML, XML/XSL, PDF and more
- Supports Exchange, Outlook, Thunderbird and other popular email types, including nested and ZIP attachments
- Spider supports static and dynamic web data like ASP.NET, MS SharePoint, CMS, PHP, etc.
- API for SQL-type data, including BLOB data

25+ full-text and fielded data search options

- Federated searching
- Special forensics search options
- Advanced data classification objects

APIs for C++, Java and .NET through 4.x

- Native 64-bit and 32-bit Win / Linux APIs; .NET Spider API
- Content extraction only licenses available

With dtSearch: "Endless indexing is now a breeze"
Computerworld

"Impressive searching power ... handles more than a terabyte of text in a single index"
Network World

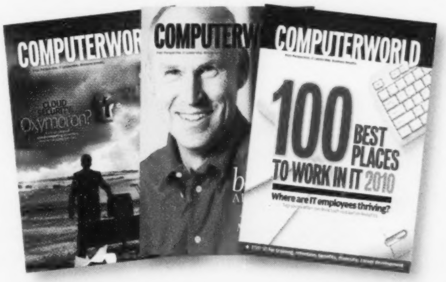
"Lightning fast ... performance was unmatched by any other product"
Redmond Magazine

For hundreds more reviews and developer case studies, see www.dtSearch.com

www.dtSearch.com • 1-800-IT-FINDS

Q: Want to reach 165,000 readers?

A: Place your ad here


COMPUTERWORLD
Oxymoron?
COMPUTERWORLD
COMPUTERWORLD
100 BEST PLACES TO WORK IN IT 2010
Where are IT employees thriving?

The Marketplace section of

COMPUTERWORLD

For more information contact:

Enku Gubaie
508.766.5487
egubaie@idgenterprise.com

We Buy Memory!

For PC, Server, and Laptop

Wanted, Call or Email now!

- 1,2,4,8 GB Desktop, Laptop, Server Memory
- Intel & AMD CPU's
- Cisco Switches

Call Jeff TODAY!

SMS MEMORY

The low price leader for quality memory modules since 1989

(239)-596-2254

JeffSMSmemory@gmail.com | www.smsassembly.com

Career Watch

© FOTOLIA / VICTOR ZASTOL'SKIY

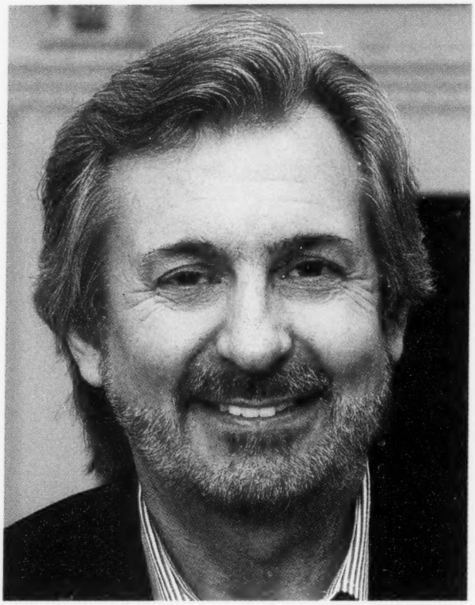
State CIOs Face Hiring Challenges

In a report titled "State IT Workforce: Under Pressure," the National Association of State Chief Information Officers took a look at the staffing challenges facing CIOs of state governments. They include hiring freezes, looming retirements of baby boomers and a decrease in interest in public sector careers among younger people. **The CIOs were also asked which specific skills present the greatest challenges when it comes to attracting and retaining IT employees.**

Skill	Percentage of CIOs who said it poses a hiring and retention challenge
Security	52.4%
Project management	50%
Application and mobile application development and support	47.6%
Architecture	47.6%
Analysis and design	42.9%
Networking support	40.5%
Infrastructure/cloud computing	31%
Web development/support	28.6%
Mainframe support	28.6%
Client/server development and support	26.2%
Contract management	23.8%
Disaster recovery/business continuity	21.4%
Testing/quality assurance	16.7%
Geospatial analysis	14.3%
Web 2.0/social media development and support	9.5%
Help desk and training	7.1%

Note: Multiple responses allowed.

SOURCE: NASCIO SURVEY OF 40 STATE CIOs, JANUARY 2011



Q&A

David Foote

The CEO of IT workforce analyst firm **Foote Partners** *says the IT workforce is larger than most of us realize.*

You maintain that government statistics on IT employment are misleading. Could you explain? Well, *statistics* and *misleading* are two words that frequently appear together, and federal employment reports raising suspicions is nothing new, especially at the start and end of recessions. But the problem with IT employment statistics is more black-and-white.

It begins with the Labor Department's Standard Occupational Classification system, which was updated in 2010 but still defines IT much the same as back in the old pure-technology MIS departments – administrators, engineers, programmers, developers, analysts, user support and various infrastructure specialists. All federal employment reports map to the SOC's ancient IT model, which means only a small portion of the modern IT professional workforce is actually identified and tracked in these reports – barely 20%, to be precise, and that's if you include tech consulting and temporary staffing jobs.

So the government doesn't see someone who oversees online security and social media development and reports to a business unit as an IT worker. Right. Nor does it properly identify and track 16 million other people in the U.S. who bring various blends of technology skills, subject matter expertise and business savvy to their jobs in corporate functions, departments, product groups, business lines and other areas. These are IT professionals in 2011. Let's face it: IT jobs and skills have been migrating outside the walls of the traditional IT department for years, from administrative to executive levels. Marketing specialists, sales engineers, business analysts, logistics experts and even vice presidents of operations can now show impressive IT résumés. The list goes on and on. You'd think the government would have heard of social media, mobile computing, data analytics, collaboration technology and ERP by now.

Why does the classification matter? It matters for two reasons. The traditional part of the IT workforce was hit pretty hard by the recession, spurring debate about whether IT is still a viable profession. But when you look at how great the other 80% of IT professionals are doing, the notion of a jobless recovery or weakness in demand for IT skills and workers is utterly ridiculous.

The intensity of the debate is the other reason why we have to get this right. As the boomers start to retire in big numbers, we can't afford to let young workers coming into the workforce mistakenly think that there aren't enormous IT job and career opportunities available to them. The bottom line is that there's never been a better time in history to be starting or building an IT career than right now, nor one with as many entry points and options. Once you grasp the reality of how much the label "IT professional" has changed, it becomes pretty obvious.

Do you think the workers see themselves as hybrids? What matters more is that their *employers* do. Even traditional IT jobs have been reshuffled and substantially redefined, with new skill requirements and aptitudes piled on, even though many times the job titles have remained unchanged. It's driving HR departments crazy, especially compensation managers who have to figure out how to pay and reward these so-called IT-business hybrid workers competitively. These are high-impact contributors you can't afford to lose, and the market for them has been red-hot for a long time.

What does all this mean for employers? It's a daunting challenge for both the public and private sectors because the role of IT in the enterprise is so pervasive that managing it is now distributed throughout the enterprise. Each group has to determine how to make the best use of IT to produce revenues and profits, build or protect market share, provide services, ensure that customers remain satisfied, control costs, innovate solutions, and generally stay competitive.

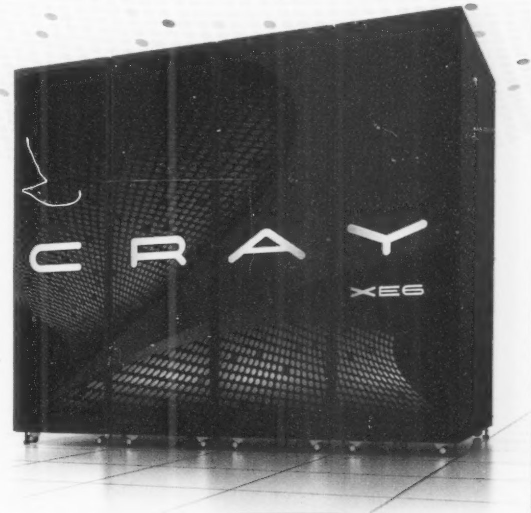
This kind of pervasive IT is at odds with organizational structures and management habits and practices that have been in place for decades. There's resistance. There's also a skills acquisition feeding frenzy happening – employers are frantically searching for people with unique combinations of knowledge, experience and skills. It's driving huge growth numbers in managed services, cloud computing, contractors, consultants and the entire services industry. At least the government got this one right: The jobs reports show more than 80,000 new jobs in the technical consulting services industry over the past 12 months.

– JAMIE ECKLE

The Way to Better Science.™

Cray builds computers that accelerate solutions to science and engineering's toughest challenges. Since 1976, Cray systems have brought unparalleled performance and processing capability, enabling countless scientific breakthroughs. And with solutions ranging from the deskside to the datacenter, Cray has the answer for you.

WWW.CRAY.COM



AMD Opteron 64

Powered by industry leading AMD Opteron™ processors

IT|careers

Computer Professionals with diff. skill sets for MD based IT Firm: Jr. Lvl. Positions – Prog. Analysts, Sys. Analysts & Bus. Analysts to Design, develop, test, create and modify computer applications s/w & specialized utility programs. Analyze user needs along with data gathered & develop sol. or alternative methods of proceeding. Manage backup & security. Sr. Lvl. Positions – Sr. Prog. Analysts, Sr. Sw. Engineers, Sr. Bus. Analysts to Design, develop, plan, coordinate & implement advance s/w module components in complex computing environments. Evaluate the organization's technology use, needs & recommend improvements in hardware & software. Plan backup & security. Travelling may be required. All professionals must be willing to relocate as necessary. Apply w/2 copies of resume to HR, Xpedite Technologies, Inc. 8830 Stanford Blvd. Ste # 314, Columbia, MD 21045

Sr. Software Engineers: Research, design, dev., code & test computer s/w systems, support & maintain existing applications & systems to determine potential areas for change & improvements. Analyze user needs, develop s/w solutions & perform unit tests etc. Sr. Programmer Analysts: Design, develop code & modify comp. applications s/w & specialized utility programs. Analyze user needs. Co-ordinate the installation, configuration & admin. of comp. programs & systems etc. Programmer Analysts & Systems Analysts: Design, develop, test, create & modify comp. applications s/w & sp. utility programs. Analyze user needs, data gathering, maintain & troubleshoot etc. Apply w/2 copies of resume to HR, Paradigm Infotech, Inc. 8830 Stanford Blvd Ste#312, Columbia, MD 21045. We are Equal opportunity employer.

Computer Professionals for (Secaucus, NJ) IT firm. JR. LVL POSITIONS: Programmer Analysts, S/w Engineers, QA analyst, Database Administrators, Systems Administrators to develop, create maintain, Test, Network & modify general comp. applications s/w or specialized utility programs, analyze user needs & develop S/w solutions. SR. LVL POSITIONS: Sr. S/w Eng, Sr. Programmer Analysts, Sr. QA Analyst, Sr. Database Administrators, Sr. Systems Administrators to maintain, administer, plan, direct, test or coordinate activities in such fields as electronic data processing, information systems, systems analysis, business analysis & comp. programming. Should be willing to travel and relocate if required. Apply w/2 copies of resume to H.R.Dept, Microexcel, Inc. One Harmon Plaza, 10th Floor, Secaucus, NJ 07094

Vice President & Head of HR (Americas). Patni Americas, Inc., an established and expanding IT consulting company with headquarters in Cambridge, MA is searching for VP, Head of HR (Americas). Qualified candidates will possess MS level education in Economics, Business or a related field and relevant industry experience. Candidates with a BS level degree and significant industry experience will be considered. HR managerial experience in the IT sector, including global employee mobility required. Position is based out of US corporate headquarters in Cambridge, MA and requires frequent business travel (both in the US and abroad) Qualified applicants submit resumes to HR Department (Attn: Mithilesh Sharma), Patni Americas, Inc., One Broadway, 15th floor, Cambridge, MA 02142.

IT Project Manager needed in NJ, AR & other unanticipated sites as DBA using DB2 UDB. Mail resume to: Collabera, Attn: Hireme, 25 Airport Rd., Morristown, NJ 07960.

Lead Technical Architect needed w/ exp using ATG & J2EE. Mail resume to REV Solutions, Attn: C. Simich, 10400 Viking Dr., #500, Eden Prairie, MN 55344.

Network & Computer Systems Administrator (Ontario,CA): Design, plan, install, administer, & maintain local area network's (LAN) hardware, software & overall network security to meet company needs. Email resume w/ CL to HR Assistant, Century Automotive Manufacturing, Inc.at calvin.wen@centuryautomfg.com

SAP Systems Administrator (Atlanta, GA opening, may relocate to unanticipated locations across the country per contract demand): Participate in SAP Implementations, Maintenance, Configuration and Integration. Fax Resume to President, Omnisoft, Inc. at 770-234-5756.

Systems Analyst (SAP/HR) sought by established IT Consulting firm. Responsible for SAP HR technology architecture, systems, software and resources across multiple modules. Position requires MS degree and at least 12 months of relevant work experience. Positon based out of Vienna, VA and subject to relocation throughout the US. Send resume to: HR Department, Supremesoft Corporation, 1608 Spring Hill Road, Suite 210, Vienna, VA 22182.

Looking for something new?

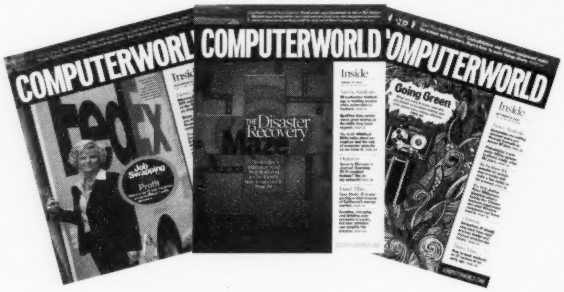
You've come to the right place!

Check back with us weekly for fresh listings placed by top companies looking for skilled professionals like you!

IT|careers

COMPUTERWORLD

Law Firms IT Consultants Staffing Agencies



Place your Labor Certification Ads Here

Are you frequently placing legal or immigration advertisements?

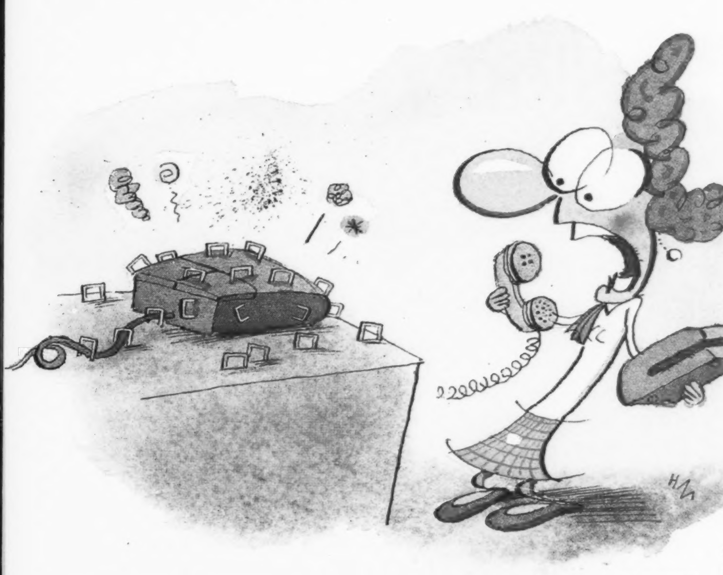
Let us help you
put together a
cost-effective program
that will make this
time-consuming
task a little easier.

Contact us at:
800.762.2977

IT|careers

SHARKTANK

TRUE TALES OF IT LIFE AS TOLD TO SHARKY



HAL MAYFORTH

Yeah, That Explains It

At the help desk for this small hospital, support pilot fish gets a call from a user who wants a new mouse. "She said her old one no longer worked," reports fish. "Thinking she just unplugged the mouse, I asked her what happened before it stopped working. She said, 'I accidentally stapled my mouse to the desk, and now I can't get it to work.' After a moment of silence, I asked her how one staples a mouse to a desk. Her reply was, 'Well, I have an electric stapler.' I decided it was best to give her the new one – with her promise that she would not use the stapler on it."

Employee Screening

Programmer pilot fish working at a local government office is writing a not-very-exciting application. "Being young and having a little evil streak in me, I linked the application to some code lifted from a computer game, which put a picture of a crack on the computer screen," fish says. "I added the code into the application at a certain point, then wrote in the manual that users should *not* press a certain key combination at that point. If the user pressed those obscure keys at that point, the program flashed the message, 'I told you not to do that!' and five seconds later put the crack on the screen. After 10 seconds the screen went back to normal, like nothing had happened. Then, no matter what the user did or how many times he tried pressing those keys, nothing would happen until one week was up. Within a week after the application went live, the users had found that feature and proceeded to use it on new trainees in their department to panic them. It just goes to show that sometimes the users *do* read the manual."

Sorry, Wrong Number

This pilot fish is responsible for supporting mobile devices for her office, including cellphones. "One user came into my office asking if I could block text messages from coming in on his cellphone," she says. "Apparently, someone he didn't know was texting him. He received a couple of text messages on Sunday and again on Monday. Not knowing who the texter was, he decided to call the phone number and let the texter know that he was sending messages to the wrong number. The phone went to voice mail, and it was one of those generic messages saying that the voice mail box for that user had not been set up, so callers couldn't leave messages. Within a couple of minutes, he gets a text: 'What the * are you doing calling me right now?? You know my wife is home!' When we called the number the next day, a man answered. We explained that he had been texting the wrong phone number, and he quickly thanked us and hung up. Problem solved."

» **Throw Sharky a line** with your true tale of IT life at sharky@computerworld.com. You'll get a stylish Shark shirt if I use it.

CHECK OUT Sharky's blog, browse the Sharkives and sign up for home delivery at **computerworld.com/sharky**.

ADVERTISERS' INDEX

This index is provided as an additional service. The publisher does not assume any liability for errors or omissions.

CDW cdw.com/adobe	5
Cisco cisco.com/go/dcbusiness	29
Citrix citrix.com/simplicityispower	16-17
Cray cray.com	39
Dell dell.com/vstart	7
dtSearch dtsearch.com	37
Hewlett-Packard hp.com/go/complexity3	C4
IBM Non-Intel ibm.com/facts	C2, 21
Microsoft microsoft.com/cloud/privatecloud	11, 12, 13
Qwest ultimateproblemsolver.com	C3
SMS Module Assembly Inc. smsassembly.com	37
SNW Spring 2011 snwusa.com	33
SunGard sungardas.com/cloud11	25
Tech Briefcase	35
Trend Micro trendmicro.com/cloud	27
VMWare vmware.com/movebeyond	3
Workday workday.com	9

BPA WORLDWIDE Periodical postage paid at Framingham, Mass., and other mailing offices. Posted under Canadian International Publication agreement PM40063731. **CANADIAN POSTMASTER:** Please return undeliverable copy to PO Box 1632, Windsor, Ontario N9A 7C9. Computerworld (ISSN 0010-4841) is published twice monthly by Computerworld Inc., 492 Old Connecticut Path, Box 9171, Framingham, Mass. 01701-9171.

Copyright 2011 by Computerworld Inc. All rights reserved.

Computerworld can be purchased on microfilm and microfiche through University Microfilms Inc., 300 N. Zeeb Road, Ann Arbor, Mich. 48106. Computerworld is indexed. Back issues, if available, may be purchased from the circulation department. Photocopy rights: permission to photocopy for internal or personal use is granted by Computerworld Inc. for libraries and other users registered with the Copyright Clearance Center (CCC), provided that the base fee of $3 per copy of the article, plus 50 cents per page, is paid directly to Copyright Clearance Center, 27 Congress St., Salem, Mass. 01970. Reprints (minimum 100 copies) and permission to reprint may be purchased from Ray Trynovich, Computerworld Reprints, c/o The YGS Group, Greenfield Corporate Center, 1808 Colonial Village Lane, Lancaster, Pa., 17601, (800) 290-5460, Ext. 148. Fax: (717) 399-8900. Web site: www.reprintbuyer.com. E-mail: computerworld@theygsgroup.com. Requests for missing issues will be honored only if received within 60 days of issue date. Subscription rates: $5 per copy: Annual subscription rates: – $129; Canada – $129; Central & So. America – $250; Europe – $295; all other countries – $295; digital subscription – $29. Subscriptions call toll-free (888) 559-7327. **POSTMASTER:** Send Form 3579 (Change of Address) to Computerworld, PO Box 3500, Northbrook, Ill. 60065-3500.

OPINION

SCOT FINNIE

Tablet Invasion

Forrester estimates that half of the first 15 million iPads are commuting to the office every day.

YOU PROBABLY THOUGHT the consumerization of IT was a big trend even before Apple sold 15 million iPads in the device's first year. Now, seemingly overnight, tablets have overrun IT. Just about every smartphone and PC maker has announced a near-iPad tablet of its own, and they're all due any day now. Gartner predicts that 69 million tablets will be sold in 2011. And here's the part that matters most to you: Forrester analyst Ted Schadler estimated in a March report on tablets in the enterprise that about half of those first 15 million iPads are commuting to the office every day.

It's inevitable, because tablets fill a need for users. No other device handles meetings as well. Tablets are light — even compared to netbooks — plus they have long battery life, and they're less off-putting to colleagues because you can type almost silently and your face isn't obscured by the display. And their screen size gives them an advantage over smartphones. Ever tried to whip out your smartphone in a meeting to check something on the Web? A phone is too small to pull down menus and press navigation buttons comfortably. What usually happens is that the conversation passes you by. A tablet like the Apple iPad or the Motorola Xoom offers a better overall design for use during meetings.

Tablets are also a good fit at companies where employees travel frequently or move about all day, and in fields like healthcare, financial services, manufacturing and retail. A tablet is an excellent small-meeting presentation device, especially in intimate settings like restaurants. And while both Forrester and IDC don't expect tablets to replace laptops, I have to wonder whether that outlook might change in a couple of years.

Challenges

Like any new platform, tablets bring with them a host of concerns for IT leaders, and you're probably not yet prepared to manage and support them in the enterprise. My advice: Don't delay.

If you haven't developed a bring-your-own-technology policy, do so now. If you have such a policy but it isn't well evolved or hasn't been well communicated to employees, get to work.

As always, you can't neglect security. It may surprise you to learn that most experts consider Apple's iOS 4.3 to be acceptably secure for typical industries, while Android still needs work. Whichever platform you use, Forrester's Schadler recommends limiting the amount of data stored on tablets (by keeping it on a server or in the cloud) for both security and e-discovery reasons.

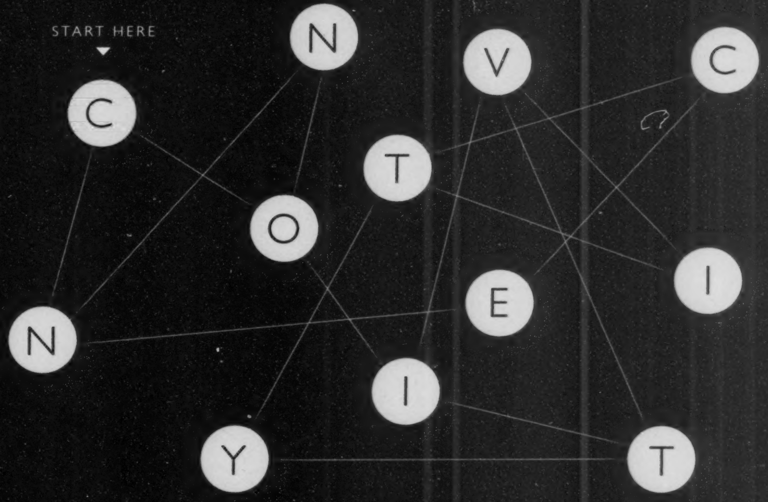
But apps, of course, are a big part of the tablet experience, so these might be the questions that enterprise IT organizations need to consider most closely: Do you go with a vendor for an enterprise app store? How do you deliver support for your internal applications? How do you handle legacy apps? (And that, by the way, might be desktop virtualization's true point of entry.) Do you build native, cross-platform or Web-based apps? Do you limit tablet support to one platform? Is HTML5 a strong part of the solution? (Not in the short run.)

Still thinking you can avoid those headaches by saying no? Then consider this: Tablets may also represent a significant customer-facing business opportunity. In a March report about tablets in business, Gartner analyst David A. Willis wrote: "If you can think of an application for tablets, your competition may well be thinking in the same way ... and acting on it."

So while you have to consider management and support, you also have to recognize that tablets could deliver significant ROI or even revenue. And you can't afford to say no to that. ◆

Scot Finnie is *Computerworld's* editor in chief. You can contact him at sfinnie@computerworld.com and follow him on Twitter (@ScotFinnie).

SOLVE *the* PROBLEM



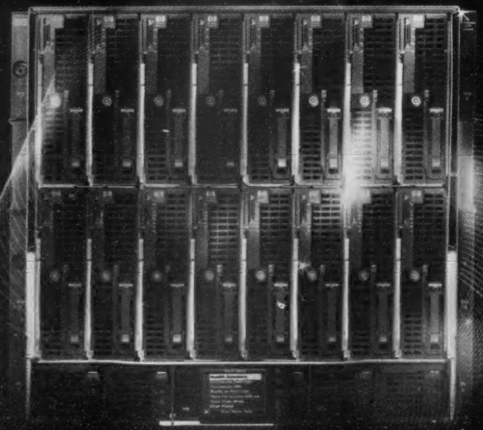
CONNECTIVITY

Disconnected workers are a problem. Unless you work with Qwest. Our innovative communication and network solutions offer seamless, scalable and easy-to-manage connectivity. With our networks you'll have secure remote access no matter how far your business takes you. The solution to this problem is your password at ultimateproblemsolver.com.

Qwest BUSINESS CenturyLink™ Business

Qwest is becoming CenturyLink.

© 2011 CenturyLink, Inc. All Rights Reserved.



AMD
Opteron™
64

UNLOCK

the possibilities of change-ready computing with the power of convergence.

HP Converged Infrastructure unlocks what's next with virtualization on HP BladeSystem.

Server virtualization has cut costs, but you can do more with the simplest way to connect to networks—HP Virtual Connect.

With HP BladeSystem featuring HP ProLiant G7 servers powered by AMD Opteron™ 6100 Series processors, HP Virtual Connect lets you wire once so you can make changes in minutes rather than days, cutting complexity and saving time.

HP Virtual Connect can deliver up to:

- 95% less network sprawl at the server edge*
- 65% cost savings on equipment*
- 40% lower power and cooling costs*

Unlock the possibilities with a free copy of *HP Virtual Connect for Dummies®*.
>> hp.com/go/complexity3

HP ProLiant BL465c G7 server

- Two twelve-core AMD Opteron™ 6100 Series processors installed
- 16GB of memory installed; expandable to 256GB
- HP Smart Array P410i Controller with 1GB Flash Backed Write Cache installed
- One integrated NC551i Dual Port 10Gb FlexFabric Converged Network Adapter
- Up to two HP hot plug small form factor SAS, SATA, or Solid State drives

$4,509 (Save $777)

Lease for just $110/mo.†

SmartBuy (PN: 630444-S01)

*For details on claim substantiations, visit hp.com/go/complexity3

†Prices shown are HP Direct prices; reseller and retail prices may vary. Prices shown are subject to change, and do not include applicable state and local taxes or shipping to recipient's address. Offers cannot be combined with any other offer or discount and are good while supplies last. All featured available offers in U.S. only. Savings based on HP published list price of configure-to-order equivalent (HP ProLiant BL465c G7 server: $5,286 -$777 = SmartBuy price $4,509). Financing available through Hewlett-Packard Financial Services Company and its subsidiaries (HPFSC) to qualified commercial customers in the U.S. and is subject to credit approval and execution of standard HPFSC documentation. Prices shown are based on a lease 48 months in term with a fair market value purchase option at the end of the term, and are valid through December 31, 2011. Other charges and restrictions may apply. HPFSC reserves the right to change or cancel this program at any time without notice.

© 2011 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

AMD, the AMD Arrow logo, AMD Opteron, and combinations thereof, are trademarks of AMD.

hp